

AT

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 06-326880

(43)Date of publication of application : 25.11.1994

(51)Int.Cl.

H04N 1/44
G09C 5/00
H04L 9/00
H04L 9/10
H04L 9/12

(21)Application number : 05-139401

(71)Applicant : MITA IND CO LTD

(22)Date of filing : 17.05.1993

(72)Inventor : SHIBATA KOICHI
OYAMA SHOICHI

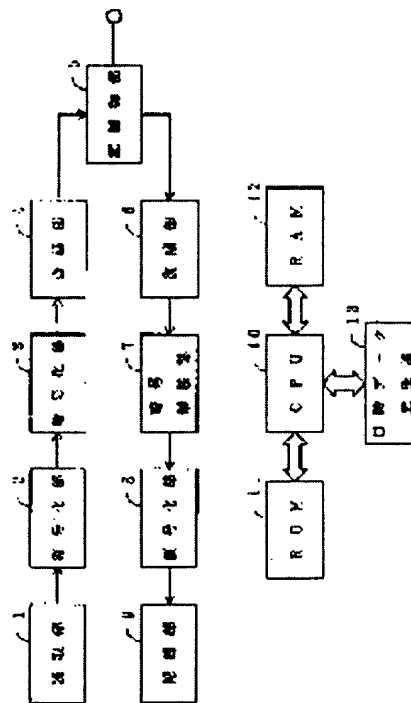
(54) CIPHERING DEVICE FOR FACSIMILE EQUIPMENT AND CIPHERING METHOD

(57)Abstract:

PURPOSE: To provide the ciphering device by which a ciphered sentence is hardly decoded by adding random data to an end of a ciphered signal so that a total bit number is a multiple of (n) thereby executing ciphering processing in the unit of n-bits.

CONSTITUTION: A read section 1 reads picture data from an original and read data are binarized. Then a coding section 2 applies MH coding to binarized data. Then a control restoration code is added to an end of a text to obtain a total bit number X of a coded signal including a control code comprising a line termination code, a fill code and a control restoration code and a remainder R dividing the bit number by a ciphering unit bit number (n) is obtained. Then random data equal to a

difference F between the ciphering unit bit number (n) and the remainder R are added after the control restoration code. The signal comprising the coded signal, control code and F-bit random data generated in this way is ciphered in the unit of n-bits by the ciphering section 3 to generate transmission data.



BEST AVAILABLE COPY

LEGAL STATUS

[Date of request for examination] 26.07.1996

[Date of sending the examiner's decision of rejection] 18.08.1998

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁(JP)

(12) 公開特許公報(A)

(11)特許出願公開番号

特開平6-326880

(43)公開日 平成6年(1994)11月25日

(51)Int.Cl. ⁵	識別記号	庁内整理番号	FI	技術表示箇所
H 0 4 N 1/44		7232-5C		
G 0 9 C 5/00		8837-5L		
H 0 4 L 9/00				
9/10				
H 0 4 L 9/00 2				
審査請求 未請求 請求項の数6 FD (全 6 頁) 最終頁に続く				

(21)出願番号 特願平5-139401

(22)出願日 平成5年(1993)5月17日

(71)出願人 000008150

三田工業株式会社

大阪府大阪市中央区玉造1丁目2番28号

(72)発明者 柴田 浩一

大阪府大阪市中央区玉造1丁目2番28号

三田工業株式会社内

(72)発明者 太山 昌一

大阪府大阪市中央区玉造1丁目2番28号

三田工業株式会社内

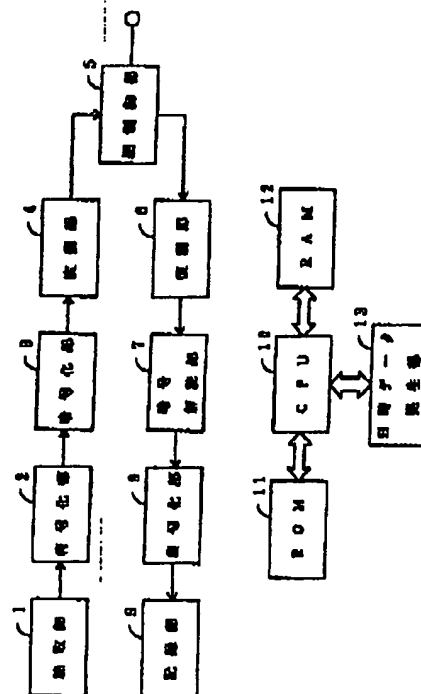
(74)代理人 弁理士 香山 秀幸

(54)【発明の名称】 ファクシミリ装置の暗号化装置および暗号化方法

(57)【要約】

【目的】 この発明は、暗号文が解読されにくいファクシミリ装置の暗号化装置および暗号化方法を提供することを目的とする。

【構成】 符号化信号に制御符号が付加された信号を被暗号化信号として、被暗号化信号をnビット単位で暗号化するファクシミリ装置の暗号化装置において、被暗号化信号の総ビット数がnの倍数であるか否かを判別する手段、および被暗号化信号の総ビット数がnの倍数でないときには、総ビット数がnの倍数となるように、被暗号化信号の最後にランダムデータを付加し、被暗号化信号にランダムデータが付加された信号をnビット単位で暗号化する手段を備えている。



(2)

特開平6-326880

2

【特許請求の範囲】

【請求項1】 符号化信号に制御符号が付加された信号を被暗号化信号として、被暗号化信号を n ビット単位で暗号化するファクシミリ装置の暗号化装置において、被暗号化信号の総ビット数が n の倍数であるか否かを判別する手段、および被暗号化信号の総ビット数が n の倍数でないときには、総ビット数が n の倍数となるように、被暗号化信号の最後にランダムデータを付加し、被暗号化信号にランダムデータが付加された信号を n ビット単位で暗号化する手段、を備えていることを特徴とするファクシミリ装置の暗号化装置。

【請求項2】 上記制御符号が各走査線の符号化の後に付加されるライン終端符号、走査線当たりの信号伝送時間が所定時間より小さい場合にライン終端符号の直前に付加されるフィル符号および1電文の最後に付加される制御復帰符号からなる請求項1記載のファクシミリ装置の暗号化装置。

【請求項3】 上記ランダムデータが日時データに基づいて作成される請求項1記載のファクシミリ装置の暗号化装置。

【請求項4】 符号化信号に制御符号が付加された信号を被暗号化信号として、被暗号化信号を n ビット単位で暗号化するファクシミリ装置の暗号化方法において、被暗号化信号の総ビット数が n の倍数でないときには、総ビット数が n の倍数となるように、被暗号化信号の最後にランダムデータを付加し、被暗号化信号にランダムデータが付加された信号を n ビット単位で暗号化することを特徴とするファクシミリ装置の暗号化方法。

【請求項5】 上記制御符号が各走査線の符号化の後に付加されるライン終端符号、走査線当たりの信号伝送時間が所定時間より小さい場合にライン終端符号の直前に付加されるフィル符号および1電文の最後に付加される制御復帰符号からなる請求項4記載のファクシミリ装置の暗号化方法。

【請求項6】 上記ランダムデータが日時データに基づいて作成される請求項4記載のファクシミリ装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】この発明は、ファクシミリ装置の暗号化装置および暗号化方法に関する。

【0002】

【従来の技術】ファクシミリ装置では、読み取られた画像信号が、MH (Modified Hoffman)、MR (Modified READ) 符号化等により符号化された後、送信される。ファクシミリ装置において、送信信号から元の信号が解読されないようにするために、符号化信号をさらに暗号化して送信することが考えられる。暗号化は、通常 n ビット単位で行われ、 n ビットの信号が n ビットの暗号化信号に変換される。

【0003】ところで、MH、MR符号化等を採用したファクシミリ装置では、符号化信号に次のような制御符号が付加される。すなわち、各走査線の符号化信号の後にライン終端符号 (EOL) が付加される。ライン終端符号は"0000000000001"の12ビットデータである。

【0004】また、走査線当たりの信号伝送時間がCCITTで定められている最小時間より小さい場合には、"0"ビットが必要数、ライン終端符号 (EOL) の直前に付加される。ライン終端符号 (EOL) の直前に付加される符号をフィル符号ということにする。

【0005】さらに、1電文の最後に制御復帰符号 (RTC) が付加されて送信される。この制御復帰符号は、ライン終端符号 (EOL) が6つ連続したものであり、"0000000000001"のパターンが6回繰り返されたデータとなる。すなわち $12 \times 6 = 72$ ビットの定型パターンが1電文の最後に付加されることになる。

【0006】

【発明が解決しようとする課題】符号化信号に、ライン終端符号 (EOL)、フィル符号および制御復帰符号 (RTC) が付加された信号を、 n ビット単位で暗号化する場合を想定する。被暗号化信号のビット数が n の倍数でない場合には、 n の倍数に不足するビット数分の"0"を付加することが考えられる。

【0007】しかしながら、このようにすると、 n の倍数に不足するビット数が多くなると、被暗号化信号の最後の n ビットの内容が知られてしまう。たとえば、 $n = 100$ で、 n の倍数に不足するビット数が38 ($= 100 - 72$) 以上になると、被暗号化信号の最後の n ビットは、ライン終端符号 (EOL) と、複数の"0"ビットとから構成され、被暗号化信号の最後の n ビットの内容が知られてしまう。そうすると、被暗号化信号の最後の n ビットと対応する暗号文とに基づいて、暗号化規則が容易に求められ、暗号文が解読され易いという問題がある。

【0008】この発明は、暗号文が解読されにくいファクシミリ装置の暗号化装置および暗号化方法を提供することを目的とする。

【0009】

【課題を解決するための手段】この発明によるファクシミリ装置の暗号化装置は、符号化信号に制御符号が付加された信号を被暗号化信号として、被暗号化信号を n ビット単位で暗号化するファクシミリ装置の暗号化装置において、被暗号化信号の総ビット数が n の倍数であるか否かを判別する手段、および被暗号化信号の総ビット数が n の倍数でないときには、総ビット数が n の倍数となるように、被暗号化信号の最後にランダムデータを付加し、被暗号化信号にランダムデータが付加された信号を n ビット単位で暗号化する手段を備えていることを特徴

(3)

特開平6-326880

とする。

【0010】この発明によるファクシミリ装置の暗号化方法は、符号化信号に制御符号が付加された信号を被暗号化信号として、被暗号化信号を n ビット単位で暗号化するファクシミリ装置の暗号化方法において、被暗号化信号の総ビット数が n の倍数でないときには、総ビット数が n の倍数となるように、被暗号化信号の最後にランダムデータを付加し、被暗号化信号にランダムデータが付加された信号を n ビット単位で暗号化することを特徴とする。号化方法。

【0011】上記制御符号は、各走査線の符号化の後に付加されるライン終端符号、走査線当たりの信号伝送時間が所定時間より小さい場合にライン終端符号の直前に付加されるフィル符号および1電文の最後に付加される制御復帰符号からなる。上記ランダムデータは、例えば、日時データに基づいて作成される。

【0012】

【作用】被暗号化信号の総ビット数が n の倍数でないときには、総ビット数が n の倍数となるように、被暗号化信号の最後にランダムデータが付加され、被暗号化信号にランダムデータが付加された信号が n ビット単位で暗号化される。

【0013】

【実施例】以下、図面を参照して、この発明の実施例について、説明する。

【0014】図1は、ファクシミリ装置の概略構成を示している。

【0015】ファクシミリ装置は、原稿画像を読み取る読取部1、読み取った画像データを符号化する符号化部2、ライン終端符号(EOL)、フィル符号および制御復帰符号(RTC)からなる制御符号が符号化信号に付加された後の信号を n ビット単位で暗号化して暗号文を作成する暗号化部3、暗号文を復調する復調部4、復調部4の出力を送信するための編制御部(NCU)5、編制御部5で受信された信号を復調する復調部6、復調部6から出力される暗号文を復調して符号化信号に戻す暗号復調部7、暗号復調部7から出力される符号化信号を復号化する復号化部8、復号化された信号に基づいて、画像データを記録紙に記録する記録部8およびこれら各部を制御する中央処理装置(CPU)10を備えている。

【0016】CPU10は、そのプログラム等を記憶するROM11、必要なデータを記憶するRAM12および日時データ発生部13を備えている。

【0017】図2は、ファクシミリ装置による送信動作を示している。

【0018】まず、読取部1によって原稿から画像データが読み取られ、読み取りデータが2値化される(ステップ1)。次に、符号化部2によって、2値化データがMH符号化される(ステップ2)。この際、各走査線の

符号化信号の後にライン終端符号(EOL)が付加される。また、走査線当たりの信号伝送時間がCCITTで定められている最小時間より小さい場合には、“0”ビットが必要数、ライン終端符号(EOL)の直前に付加される。ライン終端符号(EOL)の直前に付加される符号をフィル符号ということにする。

【0019】次に、1電文の最後に、制御復帰符号(RTC)が付加される(ステップ3)。次に、ライン終端符号(EOL)、フィル符号および制御復帰符号(RTC)からなる制御符号を含む符号化信号の総ビット数 X を、暗号化単位ビット数 n で除算したときの余り R が求められる。また、暗号化単位ビット数 n と余り R との差 F が求められる(ステップ4)。

【0020】次に、余り R が0であるか否かが判別される(ステップ5)。余り R が0でないときには、ステップ4で求められた暗号化単位ビット数 n と余り R との差 F に等しいビット数分のランダムデータが、制御復帰符号(RTC)の後に付加される(ステップ6)。

【0021】ランダムデータは、例えば日時データ発生部13から発生する日時データから作成される。たとえば、日時が10月23日13時46分であるときには、「10231346」を10進数として、この10進数を2進化して24ビットの2進数を作成する。そして、この24ビットの2進数から F ビット分のデータを取り出して、ランダムデータとする。 F が24より大きいときには、上記2進数を2乗または3乗というように m 乗して、 F よりビット数の多い2進数を作成し、作成した2進数から F ビット分のデータを取り出して、ランダムデータとする。

【0022】乱数発生器を設けて乱数発生器からランダムデータを発生させてもよい。また、ROM11に予めランダムデータとして用いるデータを記憶させておいてもよい。

【0023】このようにして作成された、符号化信号、制御符号および F ビットのランダムデータから構成される信号が、暗号化部3で n ビット単位で暗号化されて、送信用データが作成される(ステップ7)。暗号化方法としては、たとえば、 n ビット単位の被暗号化信号と n ビットの暗号用データとの対応するビットどうしの排他的論理和をとって、暗号文を作成する方法が用いられる。

【0024】上記ステップ5において、余り R が0のときには、符号化信号と制御符号とから構成される信号が、暗号化部3で n ビット単位で暗号化される(ステップ8)。また、この場合には、暗号文に、 n ビット分のランダムデータが付加されて、送信用データが作成される(ステップ9)。このランダムデータとしては、上述したように日時データから作成されたデータ、乱数発生器によって発生させたデータ、ROM11に予め記憶されたデータ等を用いることができる。

(4)

特開平6-326880

【0025】ステップ7またはステップ9で作成された送信用データは、変調部4で変調された後（ステップ10）、網制御部5を介して送信される（ステップ11）。

【0026】暗号化されたデータを受信したときの動作は、次の通りである。すなわち、網制御部5によって受信された信号は、復調部6で復調されたのち、解読部7で解読される。つまり、暗号化される前の信号に戻される。

【0027】送信側のファクシミリ装置の暗号化方法が、上述したように、 n ビット単位の被暗号化信号と n ビットの暗号用データとの対応するビットどうしの排他的論理和をとって、暗号文を作成する方法である場合には、暗号化に用いられた暗号化用データと同じ暗号化用データを用いて、暗号文が解読される。つまり、解読部7に送られてきた信号と、その信号の暗号化のために用いられた暗号用データとの排他的論理和をとることにより、解読部7に送られてきた信号が暗号化前の信号に戻される。

【0028】暗号解読部7で解読された信号は、上記ステップ6で付加された F ビット分のランダムデータまたは上記ステップ9で付加された n ビット分のランダムデータの解読信号を含んでいるが、1画文の終了は制御復帰符号（RTC）を検出することにより検知されるので、上記ステップ6または9でランダムデータが付されたことによって受信側ファクシミリ装置に悪影響を与えることはない。

【0029】暗号解読部7で解読された信号は、復号化部8で復号化された後、記録部9に送られる。そして、記録部9により、画像データが記録紙に記録される。

【0030】上記実施例では、上記ステップ5において余り R が0と判別されたときには、符号化信号と制御符号とから構成される信号が、暗号化された後に、 n ビット分のランダムデータが付加されているが（ステップ8、9参照）、余り R が0と判別されたときに、符号化信号と制御符号とから構成される信号に n ビット分のランダムデータを付加してから、暗号化を行うようにしてもよい。

【0031】また、余り R が0と判別されたときには、

符号化信号と制御符号とから構成される信号を暗号化した後、 n ビット分のランダムデータを付加することなく、暗号文を変調して送信するようにしてもよい。

【0032】上記実施例によれば、制御符号を含む符号化信号の総ビット数 X が暗号化単位ビット数 n の倍数でないときに、暗号文が解読されにくくなる。

【0033】ところで、暗号化単位ビット数 n が制御復帰符号（RTC）のビット数（72ビット）より小さくかつ制御符号を含む符号化信号の総ビット数 X が暗号化単位ビット数 n の倍数であるときにおいて、単に符号化信号と制御符号とからなる信号を暗号化するだけでは、暗号文の最後の n ビットに対する暗号化前の信号が簡単に知られてしまう。そこで、上記実施例では、制御符号を含む符号化信号の総ビット数 X が暗号化単位ビット数 n の倍数であるときには、 n ビット数分のランダムデータが暗号文に付加されて送信されているのである。

【0034】

【発明の効果】この発明によれば、暗号文が解読されにくいファクシミリ装置の暗号化装置および暗号化方法が得られる。

【図面の簡単な説明】

【図1】ファクシミリ装置の概略構成を示す電気ブロック図である。

【図2】送信時のファクシミリ装置の動作を説明するためのフローチャートである。

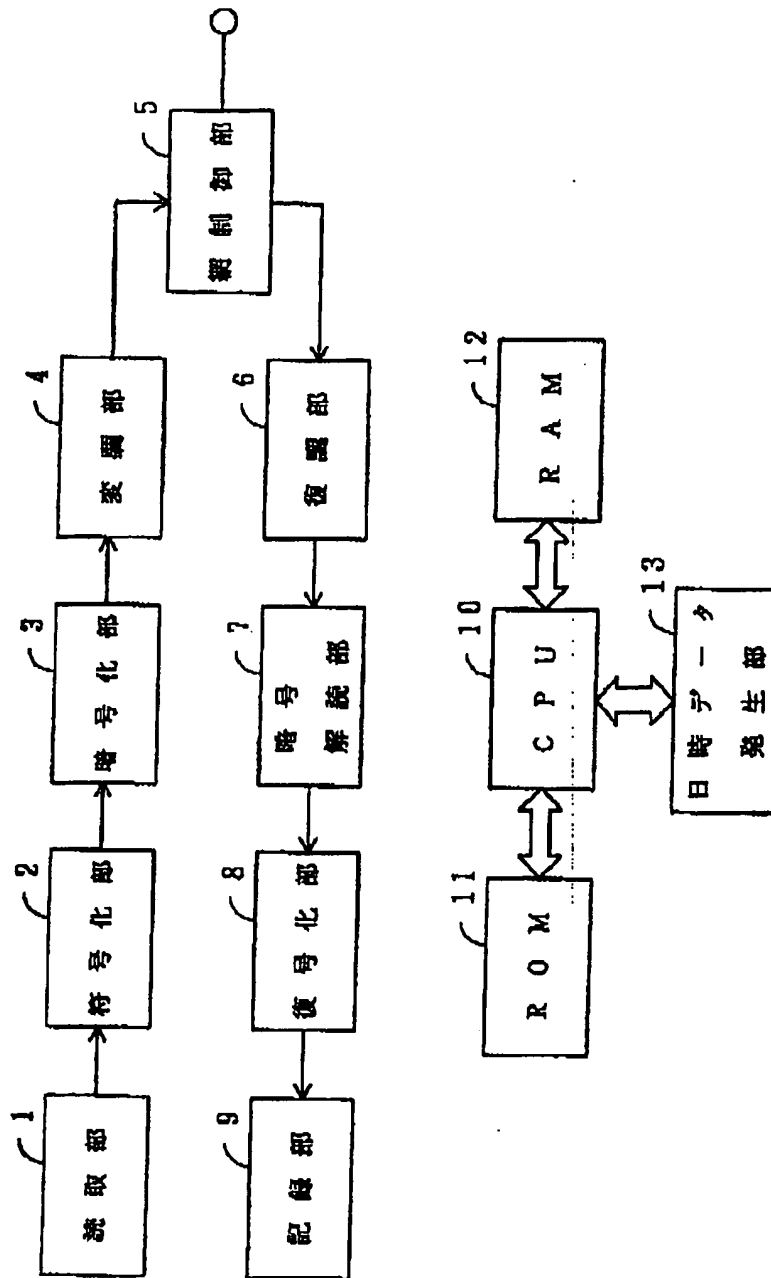
【符号の説明】

- 1 読取部
- 2 符号化部
- 3 暗号化部
- 4 変調部
- 5 NCU
- 6 復調部
- 7 暗号解読部
- 8 復号化部
- 9 記録部
- 10 CPU
- 11 ROM
- 12 RAM
- 13 日時データ発生部

(5)

特開平6-326880

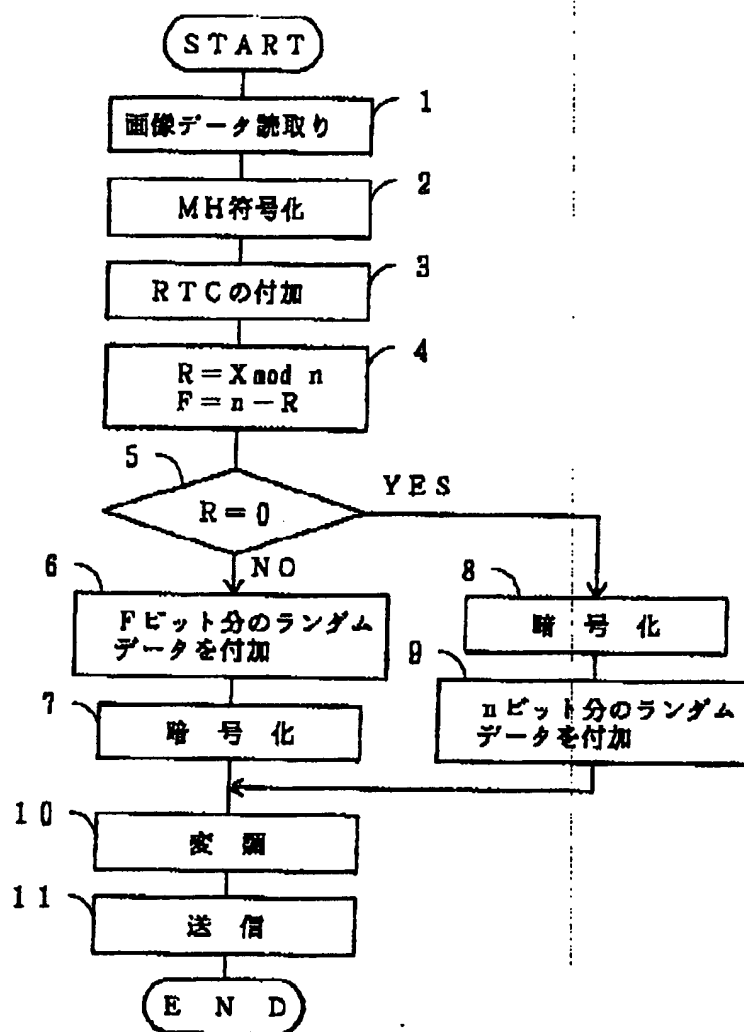
【図1】



(6)

特開平6-326880

【図2】



フロントページの続き

(51) Int. Cl. 6

識別記号

庁内整理番号

FI

技術表示箇所

H04L 9/12



Europäisches Patentamt
European Patent Office
Office européen des brevets



Publication number: **0 625 845 A1**

EUROPEAN PATENT APPLICATION

(21) Application number: 94107651.5

(51) Int. Cl.⁵: H04N 1/44, H04L 9/06

(22) Date of filing: 17.05.94

(30) Priority: 17.05.93 JP 139401/93
17.05.93 JP 139402/93

(40) Date of publication of application:
23.11.94 Bulletin 94/47

(64) Designated Contracting States:
DE FR GB IT

(71) Applicant: MITA INDUSTRIAL CO., LTD.
2-28, 1-chome, Tamatsukuri
Chuo-ku
Osaka 540 (JP)

(72) Inventor: Shibata, Koichi, c/o Mita Industrial

Co., Ltd.
2-28 Tamatsukuri, 1-chome, Chuo-ku
Osaka, 540 (JP)
Inventor: Oyama, Masakazu, c/o Mita
Industrial Co., Ltd.
2-28 Tamatsukuri, 1-chome, Chuo-ku
Osaka, 540 (JP)

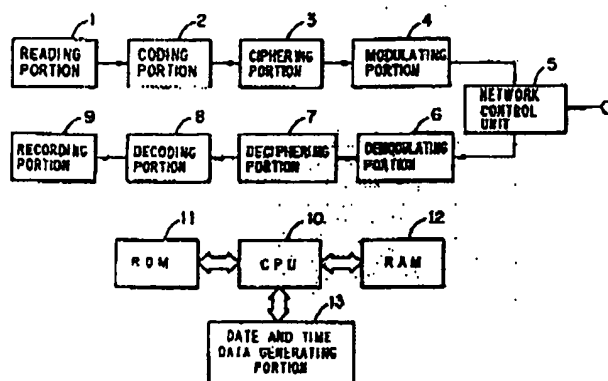
(74) Representative: Sajda, Wolf E., Dipl.-Phys. et
al
MEISSNER, BOLTE & PARTNER
Postfach 86 06 24
D-81633 München (DE)

(62) CIPHERING device and method in facsimile.

(97) A ciphering device in a facsimile apparatus is provided in which a signal to be ciphered comprising a coded signal and a control code added thereto is ciphered in units of n bits. The device comprises means for judging whether or not the total number of bits composing the signal to be ciphered is a multiple of n , and means for adding random data behind

the signal to be ciphered so that the total number of bits composing the signal to be ciphered is a multiple of n and ciphering a signal comprising the signal to be ciphered and the random data added thereto in units of n bits when the total number of bits is not a multiple of n .

FIG. 3



EP 0 625 845 A1

1

EP 0 625 845 A1

2

BACKGROUND OF THE INVENTIONField of the Invention

The present invention relates to a ciphering device and a ciphering method in a facsimile.

Description of the Prior Art

In a facsimile, an image signal read is coded by MH (modified Huffman) coding, MR (Modified READ) coding or the like and then, is transmitted. In the facsimile, it is considered that a coded signal is further ciphered and transmitted so that the original image signal is not deciphered from the transmitted signal. Ciphering processing is generally performed in units of n bits, whereby an n -bit signal is converted into an n -bit ciphered signal.

In the facsimile employing MH coding, MR coding or the like, the following control codes are added to the coded signal. Specifically, an end-of-line (EOL) code is added behind the coded signal on each scanning line. The EOL code is 12-bit data "000000000001".

Furthermore, if the signal transmission time per scanning line is smaller than the minimum time determined by CCITT, a required number of "0" bits are added just ahead of the EOL code. A code added just ahead of the EOL code shall be referred to as a FILL code.

Additionally, a return-to-control (RTC) code is added behind one telegraphic message before transmission. This RTC code is a sequence of six EOL codes "000000000001". That is, a predetermined pattern of $12 \times 6 = 72$ bits is added behind one telegraphic message.

Suppose a signal obtained by adding the control code comprising the EOL code, the FILL code and the RTC code to the coded signal is ciphered in units of n bits.

If the number of bits composing a signal to be ciphered (a plaintext) comprising the coded signal and the control code added thereto is not a multiple of n , it is considered that "0s" whose number corresponds to the number of bits which is short of a multiple of n is added.

If the number of bits which is short of a multiple of n is increased, however, the contents of the last n bits of the signal to be ciphered are estimated. For example, if $n = 100$ and the number of bits which is short of a multiple of n is not less than 38 ($= 100 - 72$), the last n bits of the signal to be ciphered is constituted by the EOL code and a plurality of "0" bits, whereby the contents of the last n bits of the signal to be ciphered are estimated. Consequently, a cipher rule is easily found on the basis of the last n bits of the signal to be ciphered and a corresponding ciphertext, so that

the ciphertext is easily deciphered.

On the other hand, merely by ciphering the signal to be ciphered comprising the coded signal and the control code when n is smaller than the number of bits (72 bits) composing the RTC code and the total number of bits composing the signal to be ciphered is a multiple of n , a signal before the ciphering corresponding to the last n bits of a ciphertext obtained by the ciphering is simply estimated. That is, a cipher rule is easily found on the basis of the last n bits of the signal to be ciphered and a corresponding ciphertext, so that the ciphertext is easily deciphered.

Examples of the cipher system includes a cipher block chaining system (abbreviated as a CBC mode). Fig. 1 shows the general construction of a CBC mode ciphering device, and Fig. 2 shows the construction of a CBC mode deciphering device.

The CBC mode ciphering device ciphers a plaintext in blocks of a predetermined number of bits, for example, in blocks of 64 bits to output a ciphertext, and further inputs for the subsequent ciphering the exclusive OR of the outputted ciphertext and a plaintext in the succeeding block.

If a plaintext is taken as M_i and a ciphertext is taken as C_i , ciphering using a cryptographic key K is taken as E_k and deciphering using the cryptographic key K is taken as D_k , CBC mode ciphering is represented by the following equations (1) and (2), and CBC mode deciphering is represented by the following equations (3) and (4):

$$C_1 = E_k (M_1 \oplus IV) \quad (1)$$

$$C_i = E_k (M_i \oplus C_{i-1}) \quad (i = 2, 3, \dots) \quad (2)$$

$$M_1 = D_k (C_1) \oplus IV \quad (3)$$

$$M_i = D_k (C_i) \oplus C_{i-1} \quad (i = 2, 3, \dots) \quad (4)$$

In the foregoing equations (1) to (4), a sign \oplus represents exclusive OR, and IV represents an initial value which is used in the case of the first ciphering and the first deciphering. The same value is used as IV in the ciphering device and the deciphering device. If the value of IV is changed, different ciphertexts are produced from the same plaintext.

If cipher communication is established according to the CBC mode, it is desirable that an initial value IV is periodically changed so as to make it difficult for a third party to decipher a ciphertext. In a facsimile on the receiving side, however, an initial value IV used in a facsimile on the transmission side must be grasped so as to decipher the received ciphertext, thereby to make it difficult to periodically change the initial value IV.

Examples of the cipher system include a secret key cipher system for performing ciphering processing using a secret key. In the secret key cipher system, ciphering processing is performed in accordance of a cipher rule for ciphering while referring to a predetermined cryptographic key. Simple examples of the cipher rule include such a rule that if plaintext data to be ciphered is taken as x , ciphertext data is taken as y , and cryptographic key data (key data) is taken as K , y is a function of $(x + K)$, i.e., $\{y = F(x + K)\}$.

If cipher communication is established according to the secret key cipher system, it is desirable that the value of key data is changed for each communication so as to make it difficult for a third party to decipher a ciphertext. In a facsimile on the receiving side, however, key data used in a facsimile on the transmission side must be grasped so as to decipher the received ciphertext, thereby to make it difficult to frequently change the key data.

SUMMARY OF THE INVENTION

A first object of the present invention is to provide a ciphering device and a ciphering method in a facsimile in which a ciphertext is not easily deciphered.

A second object of the present invention is to provide a ciphering device and a ciphering method in a facsimile in which an initial value used in a cipher block chaining system can be easily changed so that a ciphertext is not easily deciphered by a third party.

A third object of the present invention is to provide a ciphering device and a ciphering method in a facsimile in which a cryptographic key used in a secret key cipher system can be easily changed so that a ciphertext is not easily deciphered by a third party.

In a ciphering device in a facsimile in which a signal to be ciphered comprising a coded signal and a control code added thereto is ciphered in units of n bits, a first ciphering device in a facsimile according to the present invention is characterized by comprising means for judging whether or not the total number of bits composing the signal to be ciphered is a multiple of n , and means for adding random data behind the signal to be ciphered so that the total number of bits composing the signal to be ciphered is a multiple of n and ciphering a signal comprising the signal to be ciphered and the random data added thereto in units of n bits when the total number of bits is not a multiple of n .

In a ciphering method in a facsimile in which a signal to be ciphered comprising a coded signal and a control code added thereto is ciphered in units of n bits, a first ciphering method in a facsimile according to the present invention is characterized by adding random data behind the signal

to be ciphered so that the total number of bits composing the signal to be ciphered is a multiple of n and ciphering a signal comprising the signal to be ciphered and the random data added thereto in units of n bits when the total number of bits is not a multiple of n .

The above described control code comprises an EOL code added behind the coded signal on each scanning line, a FILL code added just ahead of the EOL code if the signal transmission time per scanning line is smaller than predetermined time, and an RTC code added behind one telegraphic message. The above described random data is produced on the basis of, for example, date and time data.

In the above described first ciphering device or ciphering method in a facsimile, the random data is added behind the signal to be ciphered so that the total number of bits composing the signal to be ciphered is a multiple of n and the signal comprising the signal to be ciphered and the random data added thereto is ciphered in units of n bits when the total number of bits is not a multiple of n . Therefore, a ciphertext is not easily deciphered.

In a ciphering device in a facsimile in which a signal to be ciphered comprising a coded signal and a control code added thereto is ciphered in units of n bits, a second coding device in a facsimile according to the present invention is characterized by comprising means for judging whether or not the total number of bits composing the signal to be ciphered is a multiple of n , means for ciphering the signal to be ciphered in units of n bits to produce a ciphertext when the total number of bits composing the signal to be ciphered is a multiple of n , and means for adding random data to the ciphertext to produce data to be transmitted.

In a ciphering method in a facsimile in which a signal to be ciphered comprising a coded signal and a control code added thereto is ciphered in units of n bits, a second ciphering method in a facsimile according to the present invention is characterized by ciphering the signal to be ciphered in units of n bits to produce a ciphertext when the total number of bits composing the signal to be ciphered is a multiple of n , and adding random data to the ciphertext to produce data to be transmitted.

In a ciphering device in a facsimile in which a signal to be ciphered comprising a coded signal and a control code added thereto is ciphered in units of n bits, a third ciphering device in a facsimile according to the present invention is characterized by comprising means for judging whether or not the total number of bits composing the signal to be ciphered is a multiple of n , and means for adding random data behind the signal to be

ciphered and ciphering a signal comprising the signal to be ciphered and the random data added thereto in units of n bits when the total number of bits composing the signal to be ciphered is a multiple of n .

In a ciphering method in a facsimile in which a signal to be ciphered comprising a coded signal and a control code added thereto is ciphered in units of n bits, a third ciphering method in a facsimile according to the present invention is characterized by adding random data behind the signal to be ciphered and ciphering a signal comprising the signal to be ciphered and the random data added thereto in units of n bits when the total number of bits composing the signal to be ciphered is a multiple of n .

The above described control code comprises an EOL code added behind the coded signal on each scanning line, a FILL code added just ahead of the EOL code if the signal transmission time per scanning line is smaller than predetermined time, and an RTC code added behind one telegraphic message. The above described random data is produced on the basis of, for example, date and time data.

In the above described second ciphering device or ciphering method in a facsimile, the signal to be ciphered comprising the coded signal and the control code added thereto is ciphered in units of n bits to produce a ciphertext when the total number of bits composing the signal to be ciphered is a multiple of n , and the random data is added to the ciphertext to produce the data to be transmitted. Therefore, the ciphertext is not easily deciphered.

In the above described third ciphering device or ciphering method in a facsimile, the random data is added behind the signal to be ciphered comprising the coded signal and the control code added thereto and the signal comprising the signal to be ciphered and the random data added thereto is ciphered in units of n bits when the total number of bits composing the signal to be ciphered is a multiple of n . Therefore, a ciphertext is not easily deciphered.

A fourth ciphering device in a facsimile according to the present invention is characterized by comprising ciphering means for ciphering a coded signal according to a cipher block chaining system, and initial value changing means for changing an initial value used for ciphering by the ciphering means for each predetermined time period on the basis of data concerning the calendar.

The above described data concerning the calendar includes data representing the year, data representing the month, data representing the day, data representing the time, or data comprising an arbitrary combination thereof. Examples of the

above described initial value changing means include one for determining the initial value on the basis of the date and changing the initial value for each day.

In a ciphering method in a facsimile in which a coded signal is ciphered according to a cipher block chaining system, a fourth ciphering method in a facsimile according to the present invention is characterized in that an initial value used for ciphering is changed for each predetermined time period on the basis of data concerning the calendar.

The above described data concerning the calendar includes data representing the year, data representing the month, data representing the day, data representing the time, or data comprising an arbitrary combination thereof. The above described initial value is determined on the basis of, for example, the date, and is changed for each day.

In the above described fourth ciphering device or ciphering method in a facsimile, the coded signal is ciphered according to the cipher block chaining system. The initial value used for ciphering is changed for each predetermined time period on the basis of the data concerning the calendar.

According to the above described fourth ciphering device or ciphering method in a facsimile, the initial value used in the cipher block chaining system can be easily changed, so that a ciphertext is not easily deciphered by a third party.

A fifth ciphering device in a facsimile according to the present invention is characterized by comprising ciphering means for ciphering a coded signal according to a secret key cipher system, and secret key changing means for changing a secret key used for ciphering by the ciphering means for each predetermined time period on the basis of data concerning the calendar.

The above described data concerning the calendar includes data representing the year, data representing the month, data representing the day, data representing the time, or data comprising an arbitrary combination thereof. Examples of the above described secret key changing means include one for determining the secret key on the basis of the date and changing the secret key for each day.

In a ciphering method in a facsimile in which a coded signal is ciphered according to a secret key cipher system, a fifth ciphering method in a facsimile according to the present invention is characterized in that a secret key used for ciphering is changed for each predetermined time period on the basis of data concerning the calendar.

The above described data concerning the calendar includes data representing the year, data representing the month, data representing the day, data representing the time, or data comprising an

arbitrary combination thereof. The above described secret key is determined on the basis of, for example, the date, and is changed for each day.

In the above described fifth ciphering device or ciphering method in a facsimile, the coded signal is ciphered according to the secret key cipher system. The secret key used for ciphering is changed for each predetermined time period on the basis of the data concerning the calendar.

According to the above described fifth ciphering device or ciphering method in a facsimile, the secret key used in the secret key cipher system can be easily changed, so that a ciphertext is not easily deciphered by a third party.

The foregoing and other objects, features, aspects and advantages of the present invention will become more apparent from the following detailed description of the present invention when taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram showing the construction of a CBC mode ciphering device;

Fig. 2 is a block diagram showing the construction of a CBC mode deciphering device;

Fig. 3 is an electrical block diagram showing the schematic construction of a facsimile;

Fig. 4 is a flow chart for explaining operations of the facsimile at the time of transmission;

Fig. 5 is an electrical block diagram showing the schematic construction of another facsimile;

Fig. 6 is a flow chart showing the procedure for ciphering processing performed by a control portion 101;

Fig. 7 is a flow chart showing the procedure for deciphering processing performed by the control portion 101;

Fig. 8 is a timing chart showing the relationship between an initial value used for ciphering in a facsimile on the transmission side and an initial value used in deciphering in a facsimile on the receiving side in a case where the time is around 0:00;

Fig. 9 is an electrical block diagram showing the schematic construction of still another facsimile;

Fig. 10 is a flow chart showing the procedure for ciphering processing performed by a control portion 201;

Fig. 11 is a flow chart showing the procedure for deciphering processing performed by the control portion 201; and

Fig. 12 is a timing chart showing the relationship between key data used for ciphering in a facsimile on the transmission side and key data used for deciphering in a facsimile on the receiving side in a case where the time is around 0:00.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring now to the drawings, embodiments of the present invention will be described.

Referring now to Figs. 3 and 4, a first embodiment of the present invention will be described.

Fig. 3 shows the schematic construction of a facsimile.

A facsimile comprises a reading portion 1 for reading an original image, a coding portion 2 for coding image data obtained by the reading, a ciphering portion 3 for ciphering a signal obtained by adding a control code comprising an EOL code, a FILL code and an RTC code to a coded signal in units of n bits to produce a ciphertext, a modulating portion 4 for modulating the ciphertext, a network control unit (NCU) 5 for transmitting an output of the modulating portion 4, a demodulating portion 6 for demodulating a signal received by the network control unit 5, a deciphering portion 7 for deciphering the ciphertext outputted from the demodulating portion 6 to return the same to the coded signal, a decoding portion 8 for decoding the coded signal outputted from the deciphering portion 7, a recoding portion 9 for recording the image data on recording paper on the basis of the decoded signal, and a central processing unit (CPU) 10 for controlling the respective portions.

The CPU 10 comprises a ROM 11 storing its program and the like, a RAM storing necessary data, and a date and time data generating portion 13.

Fig. 4 shows a transmitting operation performed by the facsimile.

First, image data is read from an original by the reading portion 1, and the read data is binary-coded (step 1). The binary-coded data is then subjected to MH coding by the coding portion 2 (step 2). In this case, an EOL code is added behind a coded signal on each scanning line. If the signal transmission time per scanning line is smaller than the minimum time determined by CCITT, a required number of "0" bits are added just ahead of the EOL code. A code added just ahead of the EOL code shall be referred to as a FILL code.

An RTC code is then added behind one telegraphic message (step 3). A remainder R in a case where the total number of bits X composing a signal comprising the coded signal and a control code comprising the EOL code, the FILL code and the RTC code is divided by the number of bits used as a unit for ciphering n is then found. In addition, a difference F between the number of bits used as a unit for ciphering n and the remainder R is found (step 4).

It is then judged whether or not the remainder R is zero (step 5). When the remainder R is not

9

EP 0 625 845 A1

10

zero, random data corresponding to the number of bits equal to the difference F between the number of bits used as a unit for ciphering n and the remainder R which is found in the step 4 is added behind the RTC code (step 6).

The random data is produced from, for example, date and time data generated from the date and time data generating portion 13. For example, when the date and time is October 23 and 13:46, "10231346" is taken as a decimal number, and the decimal number is binary-coded to produce a binary number composed of 24 bits. Data composed of F bits is taken out of the binary number composed of 24 bits as random data. When F is larger than 24, the binary number is multiplied by m , for example, 2 or 3, to produce a binary number composed of a larger number of bits than F , and data composed of F bits is taken out of the produced binary number as random data.

A random number generator may be provided to generate random data. In addition, data used as the random data may be previously stored in the ROM 11.

A signal comprising the coded signal, the control code and the random data composed of F bits which are thus produced is ciphered in units of n bits in the ciphering portion 3, to produce data to be transmitted (step 7). Examples of a ciphering method include a method of calculating exclusive OR of corresponding bits of a signal to be ciphered in units of n bits and n -bit data used for ciphering to produce a ciphertext.

When the remainder R is zero in the foregoing step 5, the signal comprising the coded signal and the control code is ciphered in units of n bits in the ciphering portion 3 (step 8).

In this case, the random data composed of n bits is added to the ciphertext, to produce data to be transmitted (step 9). The data produced from the date and time data, the data generated by the random number generator, the data previously stored in the ROM 11, and the like can be used as the random data.

The data to be transmitted which is produced in the step 7 or 9 is modulated in the modulating portion 4 (step 10) and then, is transmitted through the network control unit 5 (step 11).

The operation performed when ciphered data is received is as follows. Specifically, the signal received by the network control unit 5 is demodulated in the demodulating portion 6 and then, is deciphered in the deciphering portion 7. That is, the received signal is returned to the signal before the ciphering.

If a ciphering method in a facsimile on the transmission side is the above described method of calculating exclusive OR of corresponding bits of a signal to be ciphered in units of n bits and n -bit

data used for ciphering to produce a ciphertext, the ciphertext is deciphered using the same data as the data used for ciphering.

Specifically, the signal sent to the deciphering portion 7 is returned to the signal before the ciphering by calculating exclusive OR of the signal sent to the deciphering portion 7 and the data used for ciphering the signal.

Although the signal deciphered by the deciphering portion 7 includes a deciphering signal of the random data composed of F bits which is added in the foregoing step 6 or the random data composed of n bits which is added in the foregoing step 9, the end of one telegraphic message is detected by detecting the RTC code, thereby not to adversely affect a facsimile on the receiving side by the addition of the random data in the foregoing step 8 or 9.

The signal deciphered in the deciphering portion 7 is decoded in the decoding portion 8 and then, is sent to the recording portion 9. The image data is recorded on recording paper by the recording portion 9.

Although in the above described embodiment, the signal comprising the coded signal and the control code is ciphered and then, the random data composed of n bits is added thereto (see steps 8 and 9) when it is judged in the foregoing step 5 that the remainder R is zero, the signal comprising the coded signal and the control code may be ciphered after the random data composed of n bits is added thereto when it is judged that the remainder R is zero.

According to the above described first embodiment, the random data is added to the signal comprising the coded signal and the control code so that the total number of bits X composing the signal comprising the coded signal and the control code is a multiple of the number of bits used as a unit for ciphering n and then, is ciphered when the total number of bits X is not a multiple of n . Therefore, the ciphertext is not easily deciphered.

Furthermore, when the total number of bits X composing the signal comprising the coded signal and the control code is a multiple of the number of bits used as a unit for ciphering n , the random data composed of n bits is added to the ciphertext and is transmitted. Even when the number of bits used as a unit for ciphering n is smaller than the number of bits (72 bits) composing the RTC code and the total number of bits X composing the signal comprising the coded signal and the control code is a multiple of the number of bits used as a unit for ciphering n , therefore, the ciphertext is not easily deciphered.

Referring not to Figs. 5 to 8, a second embodiment of the present invention will be described.

Fig. 5 shows the schematic construction of a facsimile.

The facsimile is controlled by a control portion 101 constituted by a microcomputer and the like. The control portion 101 comprises a date and time data generating portion 102 for generating date and time data.

Furthermore, the facsimile comprises as an input-output device of the control portion 101 a reading portion 111, a recording portion 112, an operating portion 113, a display portion 114, a coding portion 115, a decoding portion 116, a modem 117, and the like. The modem 117 is connected to a public telephone line through a network control unit (NCU) 118.

The operating portion 113 comprises various operating keys, ten-keys and the like. The contents and the like set by the operating portion 113 are displayed on the display portion 114.

The operation at the time of transmission is as follows. An original image is read by the reading portion 111 and is binary-coded. Binary-coded image data obtained is coded by the coding portion 115. A coded signal obtained is ciphered according to a cipher block chaining system (hereinafter referred to as a CBC mode) by the control portion 101.

A ciphertext produced by the control portion 101 is modulated by the modem 117. The ciphertext is sent to the public telephone line through the NCU 118, and is sent to a facsimile on the receiving side. CBC mode ciphering processing is performed on the basis of equations (1) and (2) already described:

$$C_1 = E_k (M_1 \oplus IV) \quad (1)$$

$$C_i = E_k (M_i \oplus C_{i-1}) \quad (i = 2, 3, \dots) \quad (2)$$

The operation at the time of receiving is as follows. If received data is sent to the NCU 118, the received data is demodulated by the modem 117. The data demodulated by the modem 117, that is, a ciphertext is deciphered according to the CBC mode by the control portion 101, to be returned to a plaintext.

The plaintext obtained by the control portion 101 is decoded by the decoding portion 116. Image data obtained by the decoding is recorded on recording paper by the recording portion 112. CBC mode deciphering processing is performed on the basis of equations (3) and (4) already described:

$$M_1 = D_k (C_1) \oplus IV \quad (3)$$

$$M_i = D_k (C_i) \oplus C_{i-1} \quad (i = 2, 3, \dots) \quad (4)$$

In the present embodiment, an initial value IV

used for the CBC mode ciphering (see the foregoing equations (1) and (3)) is produced on the basis of the date, and is updated for each day. However, there may, in some cases, be a difference in time set between a facsimile on the transmission side and a facsimile on the receiving side.

It is assumed herein that the time difference is within 30 minutes. If the time difference set between the facsimile on the transmission side and the facsimile on the receiving side is within 30 minutes, it is possible to prevent the impossibility of deciphering in the facsimile on the receiving side by the time difference therebetween.

Fig. 6 shows the procedure for ciphering processing performed by the control portion 101.

At the time of producing a ciphertext, an initial value IV_n is produced on the basis of date data generated from the date and time data generating portion 102 (step 101).

The initial value IV_n is found on the basis of the following equation (5) if the Christian era is taken as 4-digit data A, the month is taken as 2-digit data B, and the day is taken as 2-digit data C:

$$IV_n = 10000A + 100B + C \quad (5)$$

For example, when the date of today is January 11, 1993, the initial value IV_n is "19930111".

Coded data is then ciphered on the basis of the foregoing equations (1) and (2) (step 102). In this case, the initial value IV_n found in the foregoing step 101 is used as an initial value IV. A ciphertext obtained by the ciphering is sent to the modem 117 (step 103).

Fig. 7 shows the procedure for deciphering processing performed by the control portion 101.

It is first judged on the basis of time data generated from the date and time data generating portion 102 whether or not the receiving time is time from 23:30 to 0:30 (23:30 ≤ receiving time ≤ 0:30) (step 111).

When the receiving time is not the time from 23:30 to 0:30, an initial value IV_n is produced on the basis of data representing the date of today which is generated from the date and time data generating portion 102 (step 112). This initial value IV_n is produced on the basis of the foregoing equation (5).

A ciphertext after demodulation is then deciphered on the basis of the foregoing equations (3) and (4) (step 113). In this case, the initial value IV_n found in the foregoing step 112, that is, the initial value IV_n produced from the data representing the date of today is used as an initial value IV. A plaintext after the deciphering is sent to the decoding portion 116 (step 114).

When the receiving time is the time from 23:30 to 0:30, it is judged whether the receiving time is time from 23:30 to 0:00 ($23:30 \leq \text{receiving time} \leq 0:00$) or time from 0:00 to 0:30 ($0:00 \leq \text{receiving time} \leq 0:30$) (step 115).

When the receiving time is the time from 23:00 to 0:00, the initial value IV_n is produced on the basis of the data representing the date of today which is generated from the date and time data generating portion 102, and an initial value $IV(n+1)$ is produced on the basis of data representing the date of the next day (step 116).

A method of producing an initial value is the same as the method represented by the foregoing equation (5). Therefore, when the date of today is January 11, 1993, for example, the initial value IV_n is "19930111" and the initial value $IV(n+1)$ is "19930112".

The ciphertext is then deciphered on the basis of the foregoing equations (3) and (4) by setting the initial value IV to IV_n (step 117). It is judged on the basis of the results of the deciphering whether or not the ciphertext is normally deciphered (step 118).

In the case of coding in the coding portion 115, a 12-bit EOL code "000000000001" is added behind a coded signal on each scanning line. In addition, the number of pixels constituting each line is a predetermined number. It can be judged whether or not the ciphertext is normally deciphered by, for example, finding the first EOL code from data after the deciphering, decoding data to the EOL code and judging whether or not the number of bits after the decoding is a predetermined number.

If it is judged that the ciphertext is normally deciphered, a plaintext after the deciphering is sent to the decoding portion 116 (step 122). On the other hand, if it is judged that the ciphertext is not normally deciphered, the ciphertext is deciphered on the basis of the foregoing equations (3) and (4) by setting the initial value IV to $IV(n+1)$ (step 119). It is judged on the basis of the results of the deciphering whether or not the ciphertext is normally deciphered (step 120).

If it is judged that the ciphertext is normally deciphered, the plaintext after the deciphering is sent to the decoding portion 116 (step 122). On the other hand, if it is judged that the ciphertext is not normally deciphered, communication is stopped as a deciphering error (step 121).

When in the foregoing step 115, the receiving time is the time from 0:00 to 0:30, the initial value IV_n is produced on the basis of the data representing the date of today which is generated from the date and time data generating portion 102, and an initial value $IV(n-1)$ is produced on the basis of data representing the date of the preceding day

(step 123).

A method of producing key data is the same as the method represented by the foregoing equation (5). Therefore, when the date of today is January 12, 1993, for example, the initial value IV_n is "19930112" and the initial value $IV(n-1)$ is "19930111".

The ciphertext is then deciphered on the basis of the foregoing equation (2) by setting the initial value IV to IV_n (step 124). It is judged on the basis of the results of the deciphering whether or not the ciphertext is normally deciphered (step 125).

If it is judged that the ciphertext is normally deciphered, a plaintext after the deciphering is sent to the decoding portion 116 (step 129). On the other hand, if it is judged that the ciphertext is not normally deciphered, the ciphertext is deciphered on the basis of the foregoing equation (2) by setting the initial value IV to $IV(n-1)$ (step 126). It is judged on the basis of the results of the deciphering whether or not the ciphertext is normally deciphered (step 127).

If it is judged that the ciphertext is normally deciphered, the plaintext after the deciphering is sent to the decoding portion 116 (step 129). On the other hand, if it is judged that the ciphertext is not normally deciphered, communication is stopped as a deciphering error (step 128).

Fig. 8 shows the relationship between an initial value used for ciphering in the facsimile on the transmission side and an initial value used for deciphering in the facsimile on the receiving side in a case where the time is around 0:00.

Fig. 8 (a) shows an initial value used for ciphering against the time set in the facsimile on the transmission side. The initial value used for ciphering is switched from an initial value IVA corresponding to the date A of one day to an initial value IVB corresponding to the date B of the next day utilizing the time 0:00 as a boundary.

Fig. 8 (b) shows a case where the time set in the facsimile on the receiving side is 30 minutes later than the time set in the facsimile on the transmission side. In this case, even if the receiving time in the facsimile on the receiving side is time from 23:30 to 0:00, the transmission time in the facsimile on the transmission side is time from 0:00 to 0:30. Accordingly, an initial value IV used for ciphering is IVB .

If the receiving time is the time from 23:00 to 0:00, the initial values IV_n and $IV(n+1)$ are produced in the facsimile on the receiving side (see steps 115 and 116 in Fig. 7). That is, $IVA (= IV_n)$ and $IVB (= IV(n+1))$ are produced.

Consequently, it is judged that the results of deciphering using the initial value IVA are not normal, and it is judged that the results of deciphering using the initial value IVB are normal, so that the

15

EP 0 625 845 A1

16

results of deciphering using IVB is sent to the decoding portion 116. Fig. 8 (c) shows a case where the time set in the facsimile on the receiving side is 30 minutes earlier than the time set in the facsimile on the transmission side. In this case, even if the receiving time in the facsimile on the receiving side is time from 0:00 to 0:30, the transmission time in the facsimile on the transmission side is time from 23:00 to 0:00. Accordingly, an initial value used for ciphering is IVA.

If the receiving time is the time from 0:00 to 0:30, the initial values IVn and IV (n - 1) are produced in the facsimile on the receiving side (see steps 115 and 123 in Fig. 7). That is, IVB (= IVn) and IVA (= IV (n - 1)) are produced. Consequently, it is judged that the results of deciphering using IVB are not normal, and it is judged that the results of deciphering using IVA are normal, so that the results of deciphering using IVA are sent to the decoding portion 116.

As described in the foregoing, according to the second embodiment, the initial value used for ciphering is changed in days, thereby to make it difficult for a third party to decipher the ciphertext. In addition, the initial value used for ciphering is determined on the basis of the date, thereby to make it possible to grasp the initial value used for ciphering even in the facsimile on the receiving side. Even if the initial value used for ciphering is changed in days, therefore, it is possible to decipher the ciphertext in the facsimile on the receiving side.

Furthermore, even if there is a difference in time between the facsimile on the transmission side and the facsimile on the receiving side, it is possible to normally decipher the ciphertext in the facsimile on the receiving side within a predetermined allowable difference range.

In facsimile communication between areas which differ in time, the time set in the facsimile on the receiving side is corrected on the basis of the time difference, thereby to make it possible to decipher the ciphertext as in the above described embodiment.

Month data can be used as the initial value IV, to also change the initial value for each month. In addition, time data can be also used as the initial value IV, to also change the initial value for each hour. That is, the initial value IV can be produced on the basis of the year data, the month data, the day data, the time data or data comprising an arbitrary combination thereof.

Furthermore, the initial value IV may be produced on the basis of a predetermined function utilizing as variables the year data, the month data, the day data, the time data or the data comprising an arbitrary combination thereof.

Referring now to Figs. 9 to 12, description is made of a third embodiment of the present invention.

Fig. 9 shows the schematic construction of a facsimile.

The facsimile is controlled by a control portion 201 constituted by a microcomputer and the like. The control portion 201 comprises a date and time data generating portion 202 for generating date and time data.

Furthermore, the facsimile comprises as an input-output device of the control portion 201 a reading portion 211, a recording portion 212, an operating portion 213, a display portion 214, a coding portion 215, a decoding portion 216, a modem 217, and the like. The modem 217 is connected to a public telephone line through a network control unit (NCU) 218.

The operating portion 213 comprises various operating keys, ten-keys and the like. The contents and the like set by the operating portion 213 are displayed on the display portion 214.

The operation at the time of transmission is as follows. An original image is read by the reading portion 211 and is binary-coded. Binary-coded image data obtained is coded by the coding portion 215. A coded signal obtained is ciphered according to a secret key cipher system by the control portion 201.

A ciphertext produced by the control portion 201 is modulated by the modem 217. The ciphertext is sent to the public telephone line through the NCU 218, and is sent to a facsimile on the receiving side.

One simple example of a cipher rule used by the control portion 201 is such a rule that if plaintext data is taken as x , ciphertext data is taken as y , and cryptographic key data (key data) is taken as K , y is a function of $(x + K)$, i.e., $\{y = F(x + K)\}$.

The operation at the time of receiving is as follows. If received data is sent to the NCU 218, the received data is demodulated by the modem 217. The data demodulated by the modem 217, that is, the ciphertext is deciphered according to the secret key cipher system by the control portion 201, to be returned to a plaintext.

The plaintext obtained by the control portion 201 is decoded by the decoding portion 216. Image data obtained by the decoding is recorded on recording paper by the recording portion 212.

In the present embodiment, key data used for the ciphering is produced on the basis of the date, and is updated for each day. However, there may, in some cases, be a difference in time set between a facsimile on the transmission side and a facsimile on the receiving side. It is assumed herein that the time difference is within 30 minutes.

If the time difference set between the facsimile on the transmission side and the facsimile on the receiving side is within 30 minutes, it is possible to prevent the impossibility of deciphering in the facsimile on the receiving side by the time difference therebetween.

Fig. 10 shows the procedure for ciphering processing performed by the control portion 201.

At the time of producing a ciphertext, key data K_n is produced on the basis of date data generated from the date and time data generating portion 202 (step 201).

The key data K_n is found on the basis of the following equation (8) if the Christian era is taken as 4-digit data A , the month is taken as 2-digit data B , and the day is taken as 2-digit data C :

$$K_n = 10000A + 100B + C \quad (5)$$

For example, when the date of today is January 11, 1993, the key data K_n is "19930111".

Coded data is then ciphered using the key data K_n (step 202). A ciphertext obtained by the ciphering is sent to the modem 17 (step 203).

Fig. 11 shows the procedure for deciphering processing performed by the control portion 201.

It is first judged on the basis of time data generated from the date and time data generating portion 102 whether or not the receiving time is time from 23:30 to 0:30 ($23:30 \leq \text{receiving time} \leq 0:30$) (step 211).

When the receiving time is not the time from 23:30 to 0:30, key data K_n is produced on the basis of data representing the date of today which is generated from the date and time data generating portion 202 (step 212). This key data K_n is produced on the basis of the foregoing equation (6).

A ciphertext after demodulation is then deciphered using the key data K_n produced from the data representing the date of today (step 213). A plaintext after the deciphering is sent to the decoding portion 216 (step 214).

When the receiving time is the time from 23:30 to 0:30, it is judged whether the receiving time is time from 23:30 to 0:00 ($23:30 \leq \text{receiving time} \leq 0:00$) or time from 0:00 to 0:30 ($0:00 \leq \text{receiving time} \leq 0:30$) (step 215).

When the receiving time is the time from 23:00 to 0:00, the key data K_n is produced on the basis of the data representing the date of today which is generated from the date and time data generating portion 202, and key data $K(n+1)$ is produced on the basis of data representing the date of the next day (step 216).

A method of producing key data is the same as the method represented by the foregoing equation (6). Therefore, when the date of today is January

11, 1993, for example, the key data K_n is "19930111" and the key data $K(n+1)$ is "19930112".

The ciphertext is then deciphered using the key data K_n (step 217). It is judged on the basis of the results of the deciphering whether or not the ciphertext is normally deciphered (step 218).

In the case of coding in the coding portion 215, a 12-bit EOL code "000000000001" is added behind a coded signal on each scanning line. In addition, the number of pixels constituting each line is a predetermined number. It can be judged whether or not the ciphertext is normally deciphered by, for example, finding the first EOL code from data after the deciphering, decoding data to the EOL code and judging whether or not the number of bits after the decoding is a predetermined number.

If it is judged that the ciphertext is normally deciphered, a plaintext after the deciphering is sent to the decoding portion 216 (step 222). On the other hand, if it is judged that the ciphertext is not normally deciphered, the ciphertext is deciphered using the key data $K(n+1)$ (step 219). It is judged on the basis of the results of the deciphering whether or not the ciphertext is normally deciphered (step 220).

If it is judged that the ciphertext is normally deciphered, the plaintext after the deciphering is sent to the decoding portion 216 (step 222). On the other hand, if it is judged that the ciphertext is not normally deciphered, communication is stopped as a deciphering error (step 221).

When in the foregoing step 215, the receiving time is the time from 0:00 to 0:30, the key data K_n is produced on the basis of the data representing the date of today which is generated from the date and time data generating portion 202, and key data $K(n-1)$ is produced on the basis of data representing the date of the preceding day (step 223).

A method of producing key data is the same as the method represented by the foregoing equation (6). Therefore, when the date of today is January 12, 1993, for example, the key data K_n is "19930112" and the key data $K(n-1)$ is "19930111".

The ciphertext is then deciphered using the key data K_n (step 224). It is judged on the basis of the results of the deciphering whether or not the ciphertext is normally deciphered (step 225).

If it is judged that the ciphertext is normally deciphered, a plaintext after the deciphering is sent to the decoding portion 216 (step 229). On the other hand, if it is judged that the ciphertext is not normally deciphered, the ciphertext is deciphered using the key data $K(n-1)$ (step 226). It is judged on the basis of the results of the deciphering whether or not the ciphertext is normally deciphered.

phered (step 227).

If it is judged that the ciphertext is normally deciphered, the plaintext after the deciphering is sent to the decoding portion 216 (step 229). On the other hand, if it is judged that the ciphertext is not normally deciphered, communication is stopped as a deciphering error (step 228).

Fig. 12 shows the relationship between key data used for ciphering in the facsimile on the transmission side and key data used for deciphering in the facsimile on the receiving side in a case where the time is around 0:00.

Fig. 12 (a) shows key data used for ciphering against the time set in the facsimile on the transmission side. The key data used for ciphering is switched from key data KA corresponding to the date A of one day to key data KB corresponding to the date B of the next day utilizing the time 0:00 as a boundary.

Fig. 12 (b) shows a case where the time set in the facsimile on the receiving side is 30 minutes later than the time set in the facsimile on the transmission side. In this case, even if the receiving time in the facsimile on the receiving side is time from 23:30 to 0:00, the transmission time in the facsimile on the transmission side is time from 0:00 to 0:30. Accordingly, the key data used for ciphering is KB.

If the receiving time is the time from 23:00 to 0:00, the key data K_n and $K(n+1)$ are produced in the facsimile on the receiving side (see steps 215 and 216 in Fig. 11). That is, $KA (= K_n)$ and $KB (= K(n+1))$ are produced. Consequently, it is judged that the results of deciphering using the key data KA are not normal, and it is judged that the results of deciphering using the key data KB are normal, so that the results of deciphering using KB is sent to the decoding portion 216.

Fig. 12 (c) shows a case where the time set in the facsimile on the receiving side is 30 minutes earlier than the time set in the facsimile on the transmission side. In this case, even if the receiving time in the facsimile on the receiving side is time from 0:00 to 0:30, the transmission time in the facsimile on the transmission side is time from 23:00 to 0:00. Accordingly, the key data used for ciphering is KA.

If the receiving time is the time from 0:00 to 0:30, the key data K_n and $K(n-1)$ are produced in the facsimile on the receiving side (see steps 215 and 223 in Fig. 11). That is, $KB (= K_n)$ and $KA (= K(n-1))$ are produced. Consequently, it is judged that the results of deciphering using KB are not normal, and it is judged that the results of deciphering using KA are normal, so that the results of deciphering using KA are sent to the decoding portion 216.

As described in the foregoing, according to the third embodiment, the key data used for ciphering is changed in days, thereby to make it difficult for a third party to decipher the ciphertext. In addition, the key data used for ciphering is determined on the basis of the date, thereby to make it possible to grasp the key data used for ciphering even in the facsimile on the receiving side. Even if the key data used for ciphering is changed in days, therefore, it is possible to decipher the ciphertext in the facsimile on the receiving side.

Furthermore, even if there is a difference in time between the facsimile on the transmission side and the facsimile on the receiving side, it is possible to normally decipher the ciphertext in the facsimile on the receiving side within a predetermined allowable difference range.

In facsimile communication between areas which differ in time, the time set in the facsimile on the receiving side is corrected on the basis of the time difference, thereby to make it possible to decipher the ciphertext as in the above described embodiment.

Month data can be used as the key data, to also change the key data for each month. In addition, time data can be used as the key data, to also change the key data for each hour. That is, the key data can be produced on the basis of the year data, the month data, the day data, the time data or data comprising an arbitrary combination thereof.

Furthermore, the key data may be produced on the basis of a predetermined function utilizing as variables the year data, the month data, the day data, the time data or the data comprising an arbitrary combination thereof.

Although the present invention has been described and illustrated in detail, it is clearly understood that the same is by way of illustration and example only and is not to be taken by way of limitation.

Claims

1. A ciphering device in a facsimile apparatus in which a signal to be ciphered comprising a coded signal and a control code added thereto is ciphered in units of n bits, comprising:

- means for judging whether or not the total number of bits composing the signal to be ciphered is a multiple of n ; and
- means for adding random data behind the signal to be ciphered so that the total number of bits composing the signal to be ciphered is a multiple of n and ciphering a signal comprising the signal to be ciphered and the random data added thereto in units of n bits when the total number of bits is not a multiple of n .

21

EP 0 625 845 A1

22

2. The ciphering device according to claim 1, wherein the control code comprises an end-of-line code added behind the coded signal on each scanning line, a FILL code added just ahead of the end-of-line code if the signal transmission time per scanning line is smaller than predetermined time, and a return-to-control code added behind one telegraphic message.
3. The ciphering device according to claim 1 or 2, wherein the random data is produced on the basis of date and time data.
4. A ciphering device in a facsimile apparatus in which a signal to be ciphered comprising a coded signal and a control code added thereto is ciphered in units of n bits, comprising:
- means for judging whether or not the total number of bits composing the signal to be ciphered is a multiple of n ,
 - means for ciphering the signal to be ciphered in units of n bits to produce a ciphertext when the total number of bits composing the signal to be ciphered is a multiple of n , and
 - means for adding random data to the ciphertext to produce data to be transmitted.
5. A ciphering device in a facsimile apparatus in which a signal to be ciphered comprising a coded signal and a control code added thereto is ciphered in units of n bits, comprising:
- means for judging whether or not the total number of bits composing the signal to be ciphered is a multiple of n ; and
 - means for adding random data behind the signal to be ciphered and ciphering a signal comprising the signal to be ciphered and the random data added thereto in units of n bits when the total number of bits composing the signal to be ciphered is a multiple of n .
6. The ciphering device according to claim 4 or 5, wherein the control code comprises an end-of-line code added behind the coded signal on each scanning line, a FILL code added just ahead of the end-of-line code if the signal transmission time per scanning line is smaller than a predetermined time, and a return-to-control code added behind one telegraphic message.
7. The ciphering device according to claim 4 or 5, wherein the random data is produced on the basis of date and time data.
8. A ciphering device in a facsimile comprising:
- ciphering means for ciphering a coded signal according to a cipher block chaining system; and
 - initial value changing means for changing an initial value used for ciphering by the ciphering means for each predetermined time period on the basis of data concerning the calendar.
9. The ciphering device according to claim 8, wherein the initial value changing means determines the initial value on the basis of the date and changes the initial value for each day.
10. A ciphering device in a facsimile apparatus comprising:
- ciphering means for ciphering a coded signal according to a secret key cipher system; and
 - secret key changing means for changing a secret key used for ciphering by the ciphering means for each predetermined time period on the basis of data concerning the calendar.
11. The ciphering device according to claim 10, wherein the secret key changing means determines the secret key on the basis of the date and changes the secret key for each day.
12. A ciphering method in a facsimile apparatus in which a signal to be ciphered comprising a coded signal and a control code added thereto is ciphered in units of n bits, comprising the step of
- adding random data behind the signal to be ciphered so that the total number of bits composing the signal to be ciphered is a multiple of n and ciphering a signal comprising the signal to be ciphered and the random data added thereto in units of n bits when the total number of bits is not a multiple of n .
13. The ciphering method according to claim 12, wherein the control code comprises an end-of-line code added behind the coded signal on each scanning line, a FILL code added just ahead of the end-of-line code if the signal transmission time per scanning line is smaller than a predetermined time, and a return-to-control code added behind one telegraphic

23

EP 0 625 845 A1

24

message.

14. The ciphering method according to claim 12 or 13, wherein the random data is produced on the basis of date and time data.

15. A ciphering method in a facsimile in which a signal to be ciphered comprising a coded signal and a control code added thereto is ciphered in units of n bits, comprising the steps of:

- ciphering the signal to be ciphered in units of n bits to produce a ciphertext when the total number of bits composing the signal to be ciphered is a multiple of n ; and
- adding random data to the ciphertext to produce data to be transmitted.

16. A ciphering method in a facsimile in which a signal to be ciphered comprising a coded signal and a control code added thereto is ciphered in units of n bits, comprising the step of:

- adding random data behind the signal to be ciphered and ciphering a signal comprising the signal to be ciphered and the random data added thereto in units of n bits when the total number of bits composing the signal to be ciphered is a multiple of n .

17. The ciphering method according to claim 15 or 16, wherein the control code comprises an end-of-line code added behind the coded signal on each scanning line, a FILL code added just ahead of the end-of-line code if the signal transmission time per scanning line is smaller than predetermined time, and a return-to-control code added behind one telegraphic message.

18. The ciphering method according to any of claims 15 to 17, wherein the random data is produced on the basis of date and time data.

19. A ciphering method in a facsimile in which a coded signal is ciphered according to a cipher block chaining system, wherein an initial value used for ciphering is changed for each predetermined time period on the basis of data concerning the calendar,

20. The ciphering method according to claim 19, wherein the initial value is determined on the

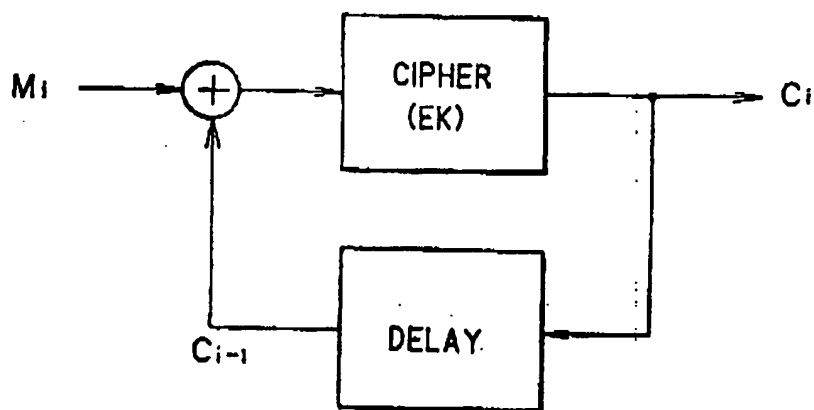
basis of the date, and is changed for each day.

21. A ciphering method in a facsimile in which a coded signal is ciphered according to a secret key cipher system, wherein a secret key used for ciphering is changed for each predetermined time period on the basis of data concerning the calendar.

22. The ciphering method according to claim 21, wherein the secret key is determined on the basis of the date, and is changed for each day.

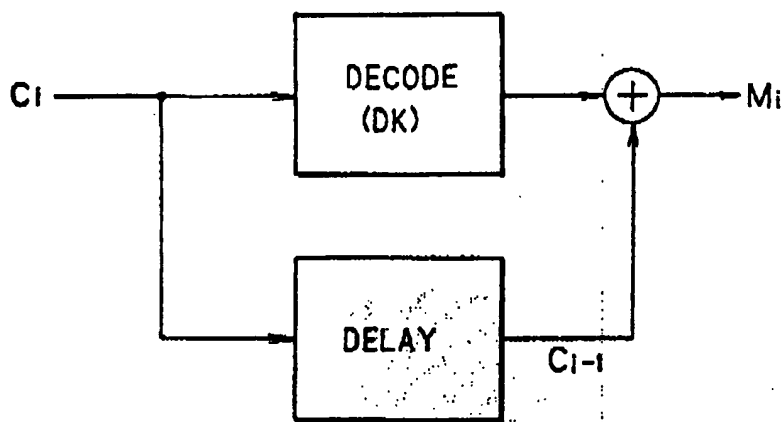
EP 0 625 845 A1

FIG. 1



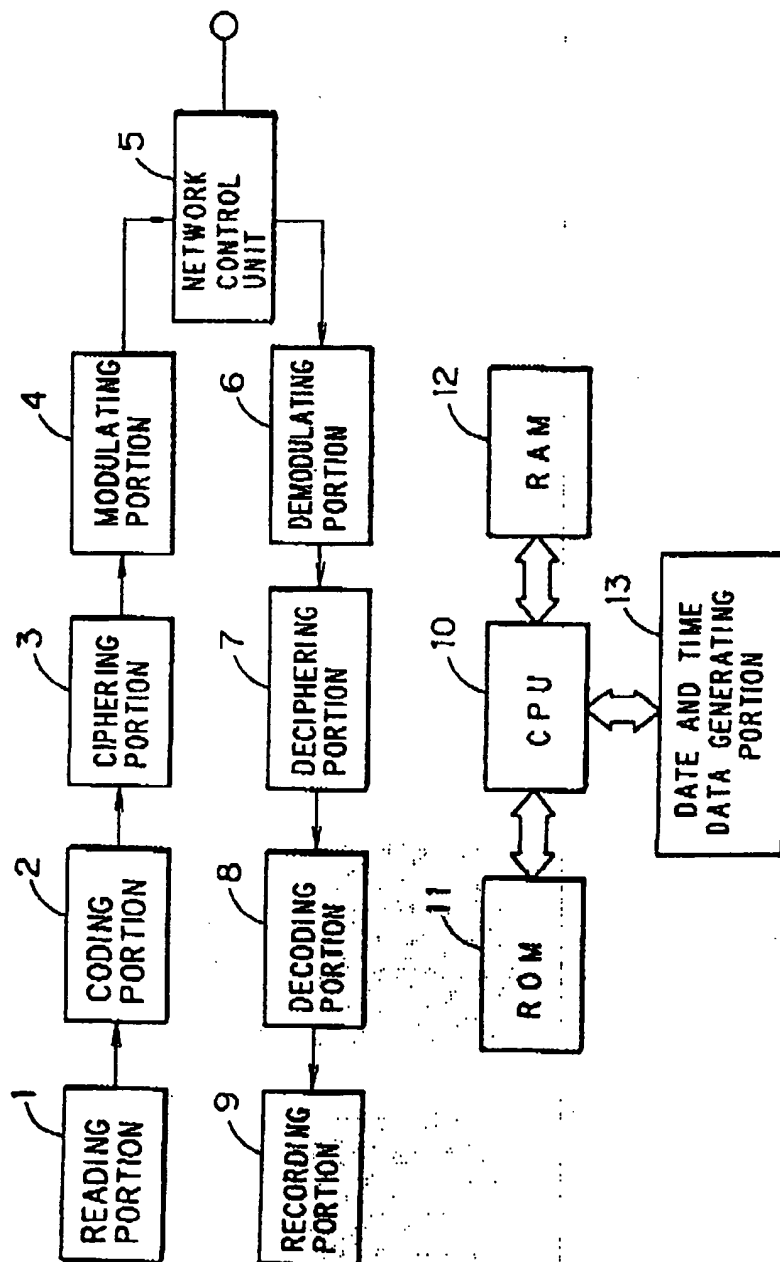
EP 0 625 845 A1

FIG. 2



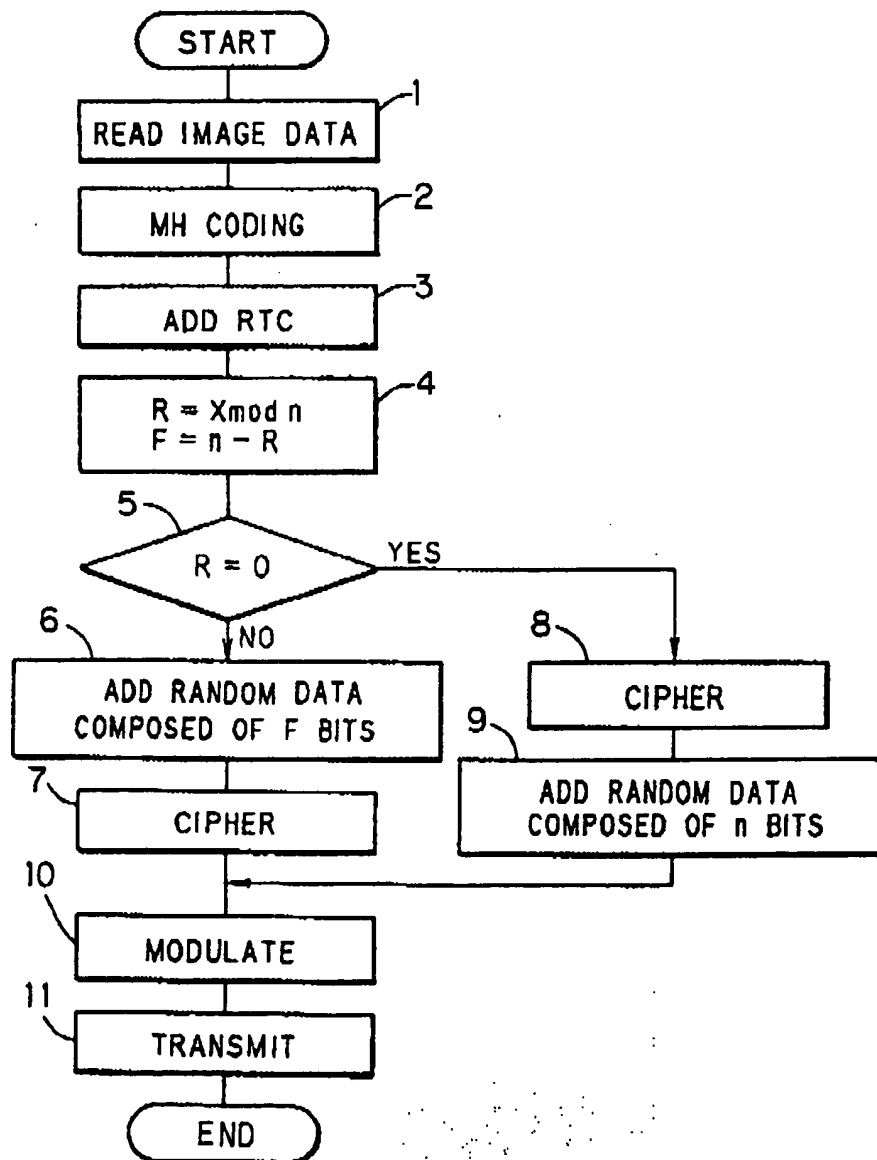
EP 0 625 845 A1

FIG. 3

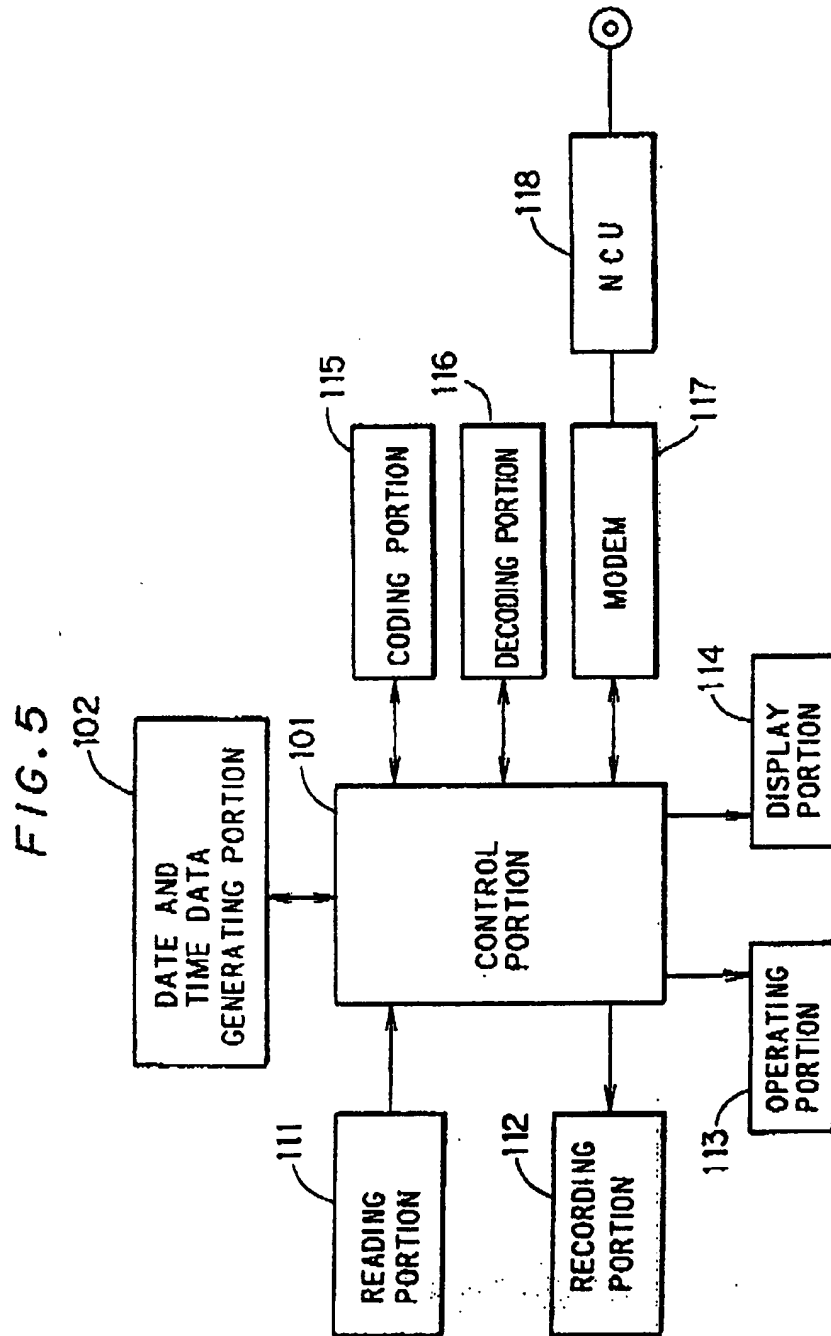


EP 0 626 845 A1

FIG. 4

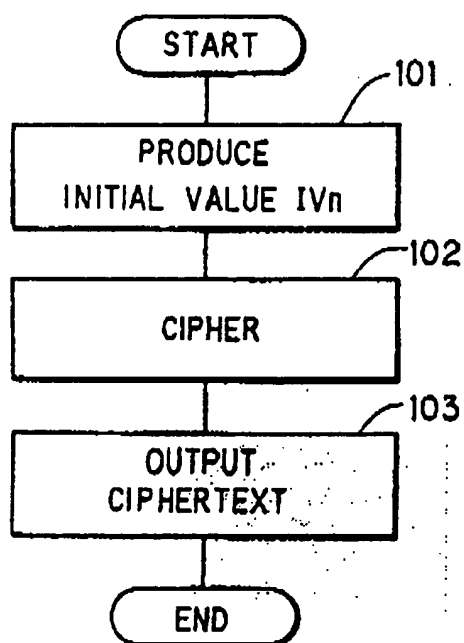


EP 0 625 845 A1



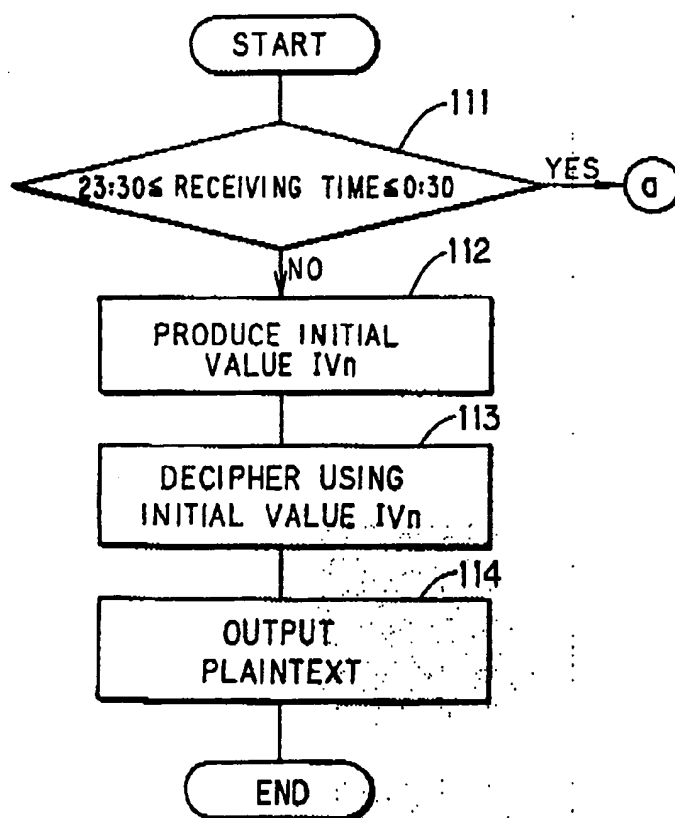
EP 0 625 845 A1

FIG. 6



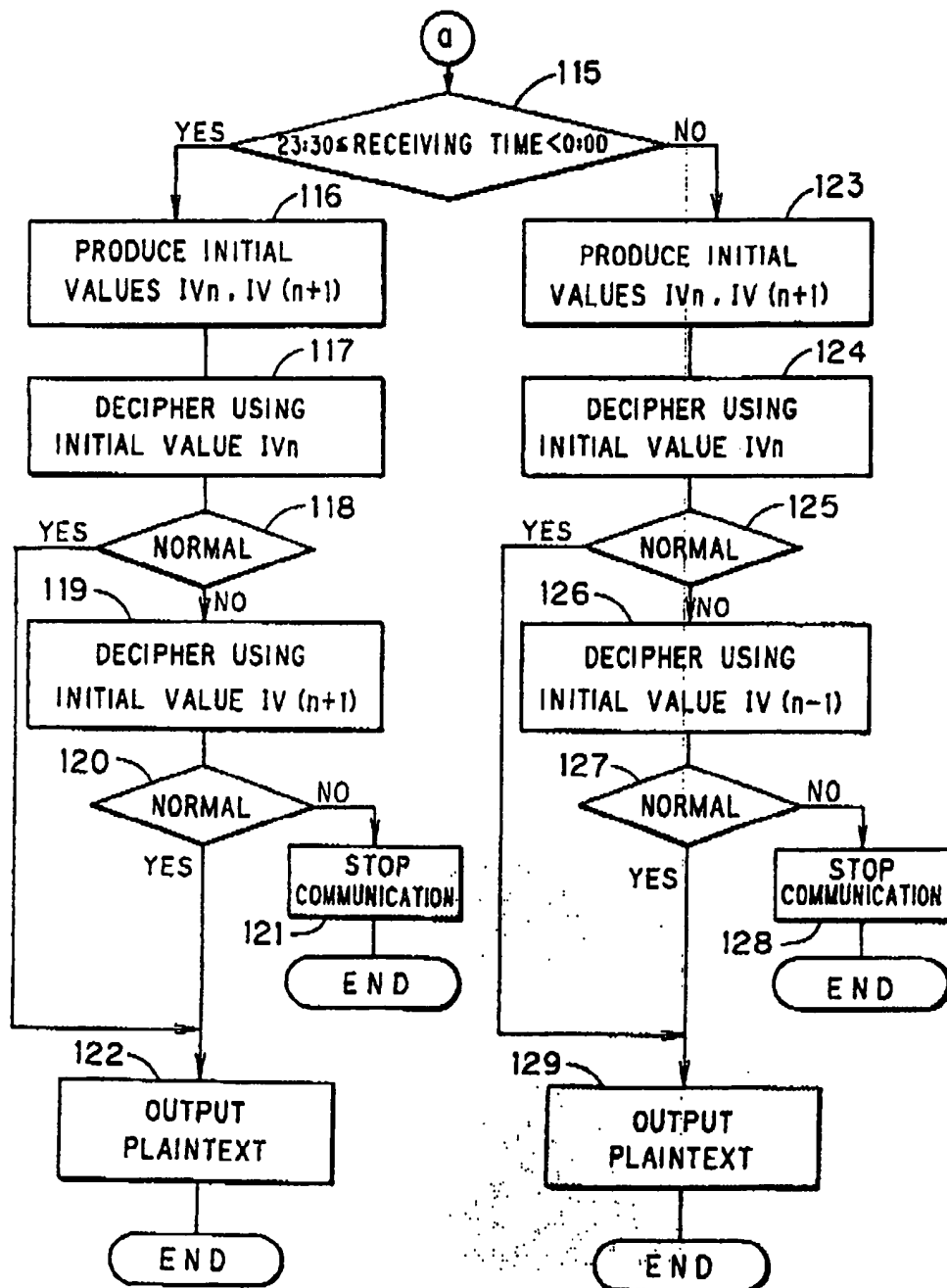
EP 0 625 845 A1

FIG. 7a



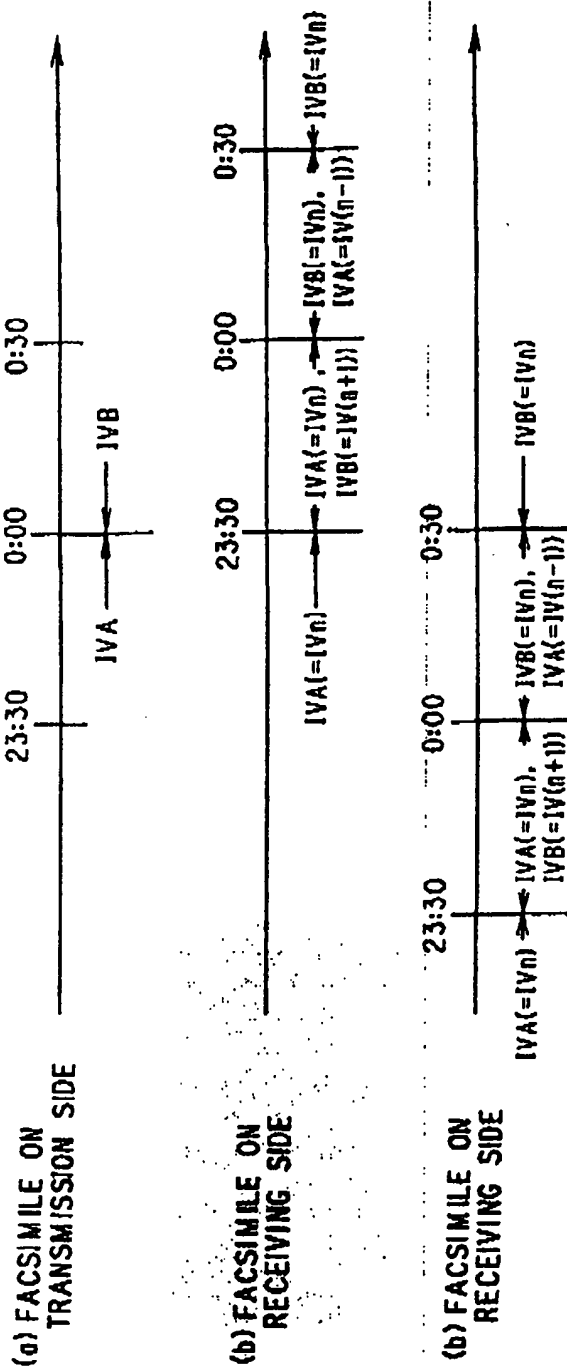
EP 0 625 845 A1

FIG. 7b



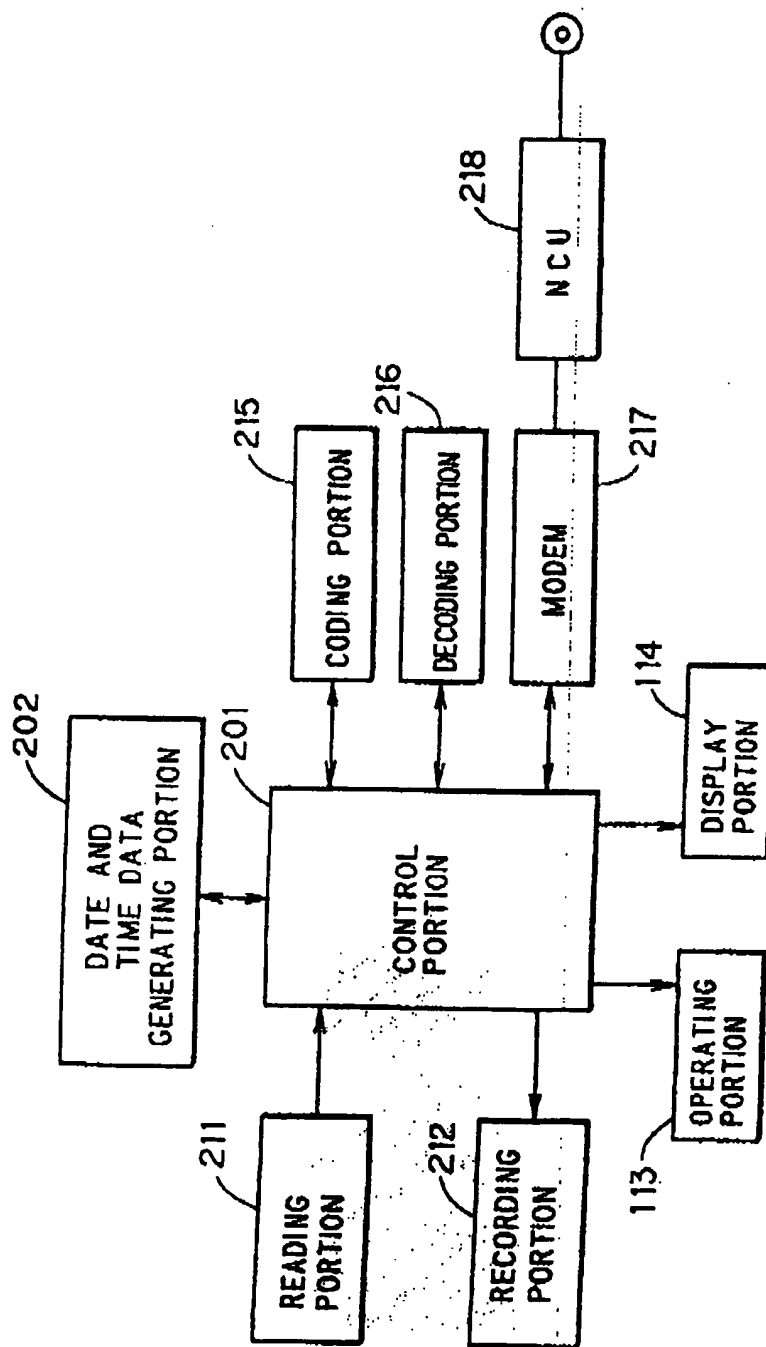
EP 0 625 845 A1

FIG. 8



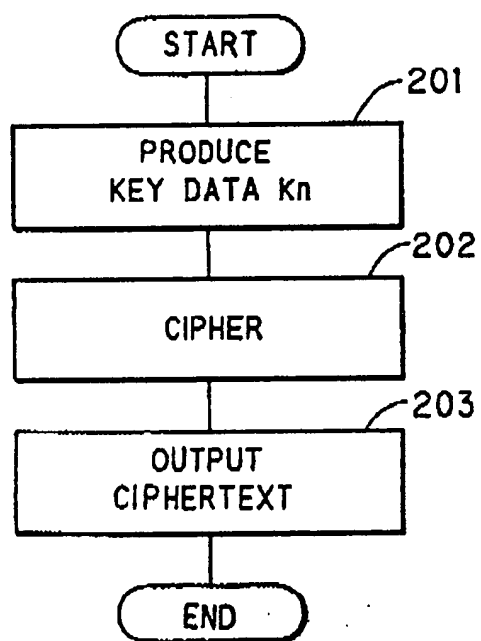
EP 0 625 845 A1

FIG. 9



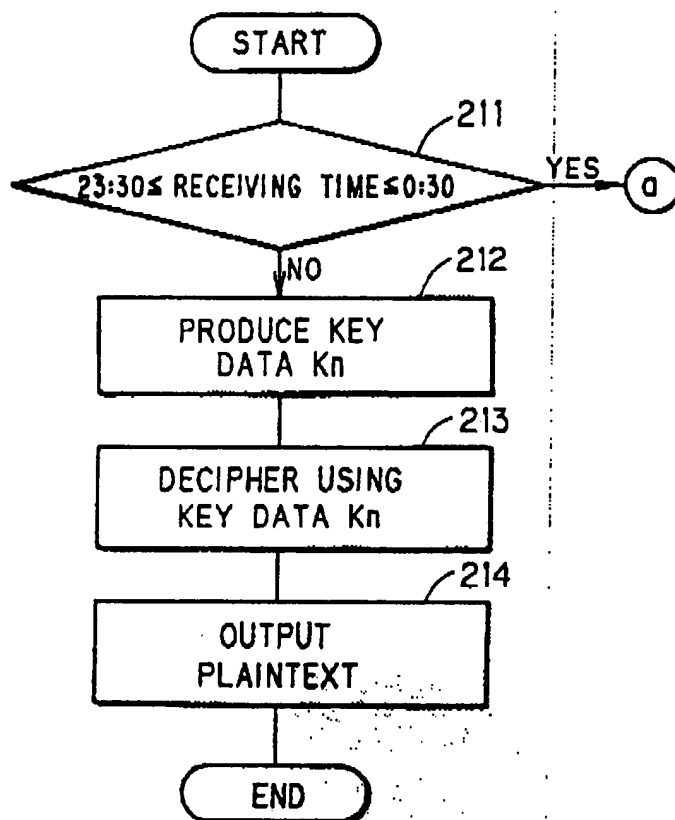
EP 0 825 845 A1

FIG. 10



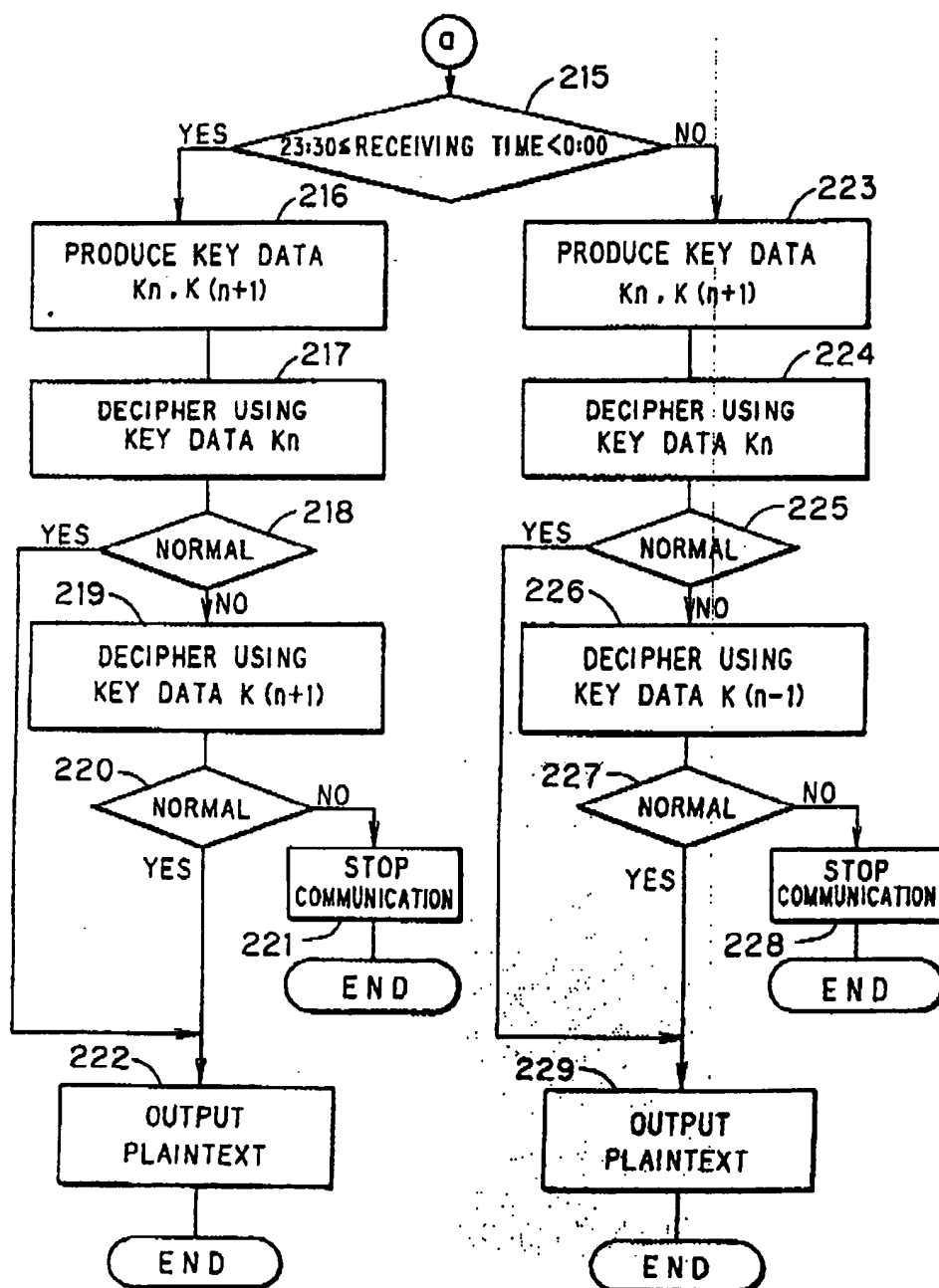
EP 0 625 845 A1

FIG. 11a



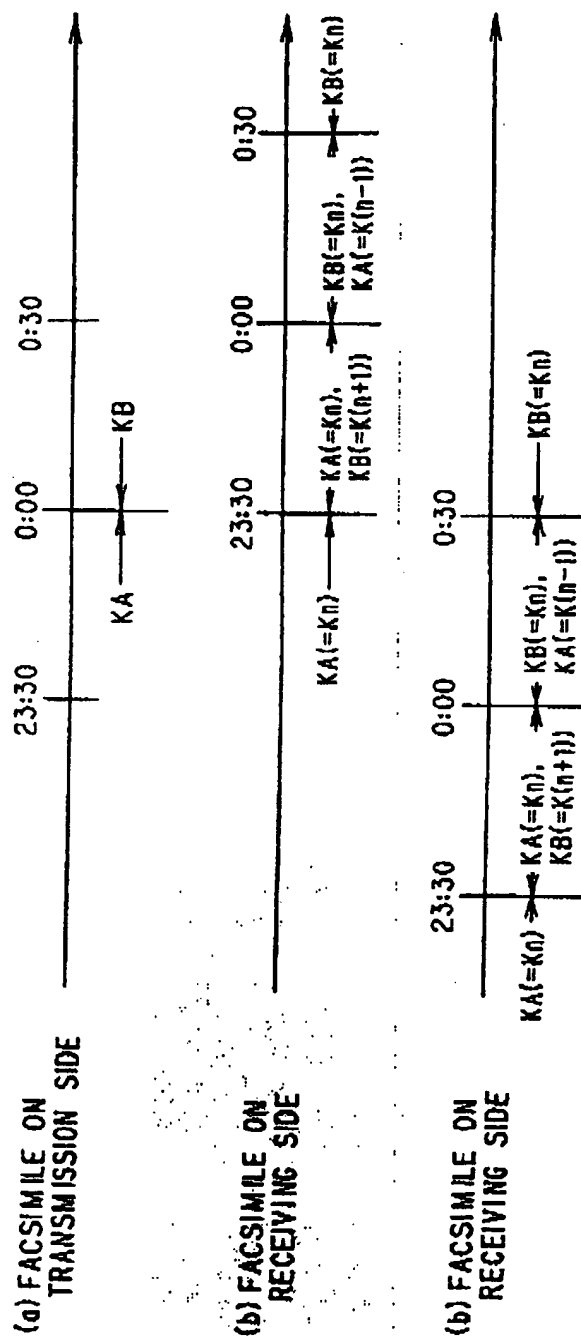
EP 0 625 845 A1

FIG. 11b



EP 0 625 845 A1

FIG. 12





European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 94 10 7651

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (In CLS)
A	COMPUTERS & SECURITY, vol.10, no.1, February 1991, OXFORD GB pages 37 - 40, XP000209186 MITCHELL AND VARADHARAJAN 'Modified Forms of Cipher Block Chaining' * page 37, left column, paragraph 2 - right column, last paragraph *	1,4,5,8, 12,15, 16,19	H04N1/44 H04L9/06
A	DE-A-31 28 414 (RICOH) * abstract *	2,6,13, 17	
A	PATENT ABSTRACTS OF JAPAN vol. 12, no. 162 (E-609) 17 May 1988 & JP-A-62 272 752 (MATSUSHITA GRAPHIC COMMUNICATION) 26 November 1987 * abstract *	2,6,13, 17	
A	FR-A-2 439 444 (LAPEYRONNIE) * page 4, line 36 - line 40 *	3,7,14, 18	TECHNICAL FIELD SEARCHED (In CLS)
P,A	PATENT ABSTRACTS OF JAPAN vol. 18, no. 105 (E-1512) 21 February 1994 & JP-A-05 304 614 (NED CORP) 16 November 1993 * abstract *	3,7,14, 18	H04N H04L
The present search report has been drawn up for all claims			
Place of search		Date of completion of the search	Examiner
THE HAGUE		10 August 1994	Isa, S
CATEGORY OF CITED DOCUMENTS		T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons A : member of the same patent family, corresponding document	
X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure F : intermediate document			

EPO FORM 500 (04/94) (PUBLISHED)

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.